J. Korean Math. Soc. **59** (2022), No. 3, pp. 621–634
https://doi.org/10.4134/JKMS.j210446
pISSN: 0304-9914 / eISSN: 2234-3008

# ON THE SCALED INVERSE OF $(x^i - x^j)$ MODULO CYCLOTOMIC POLYNOMIAL OF THE FORM $\Phi_{p^s}(x)$ OR $\Phi_{p^sq^t}(x)$

Jung Hee Cheon, Dongwoo Kim, Duhyeong Kim, and Keewoo Lee

Abstract. The scaled inverse of a nonzero element $a(x) \in \mathbb{Z}[x]/f(x)$, where $f(x)$ is an irreducible polynomial over $\mathbb{Z}$, is the element $b(x) \in \mathbb{Z}[x]/f(x)$ such that $a(x)b(x) = c \pmod{f(x)}$ for the smallest possible positive integer scale $c$. In this paper, we investigate the scaled inverse of $(x^i - x^j)$ modulo cyclotomic polynomial of the form $\Phi_{p^s}(x)$ or $\Phi_{p^sq^t}(x)$, where $p, q$ are primes with $p < q$ and $s, t$ are positive integers. Our main results are that the coefficient size of the scaled inverse of $(x^i - x^j)$ is bounded by $p - 1$ with the scale $p$ modulo $\Phi_{p^s}(x)$, and is bounded by $q - 1$ with the scale not greater than $q$ modulo $\Phi_{p^sq^t}(x)$. Previously, the analogous result on cyclotomic polynomials of the form $\Phi_{2^n}(x)$ gave rise to many lattice-based cryptosystems, especially, zero-knowledge proofs. Our result provides more flexible choice of cyclotomic polynomials in such cryptosystems. Along the way of proving the theorems, we also prove several properties of $\{x^k\}_{k\in\mathbb{Z}}$ in $\mathbb{Z}[x]/\Phi_{pq}(x)$ which might be of independent interest.

## 1. Introduction

Cyclotomic polynomials play an important role in algebra, number theory, combinatorics, and their applications. In particular, modern lattice-based cryptography intensively employs cyclotomic rings $\mathbb{Z}[x]/\Phi_M(x)$ [9, 10].

An interesting subclass of cyclotomic polynomials is of the form $\Phi_{p^sq^t}(x)$, where $p, q$ are primes with $p < q$ and $s, t$ are positive integers. Since cyclotomic polynomials of the form $\Phi_{p^s}(x)$ are just $\sum_{i=0}^{p-1} x^{ip^{s-1}}$, the case with two prime factors can be seen as the simplest non-trivial case. There have been various interesting results on these cyclotomic polynomials [2, 6, 7]. For instance, these cyclotomic polynomials have only $\{-1, 0, 1\}$ as coefficients, whereas a cyclotomic polynomial of a product of three distinct odd primes can have an arbitrarily large coefficient [8].

Received July 17, 2021; Accepted October 27, 2021.
2010 *Mathematics Subject Classification.* Primary 11C08, 94A60.
*Key words and phrases.* Cyclotomic polynomial, scaled inverse, zero-knowledge proof.
This work was supported by Samsung Electronics Co., Ltd(IO201209-07883-01). This work was done while Duhyeong Kim and Dongwoo Kim were at Seoul National University.

Benhamouda et al. [3] provided the following lemma, which was used to construct more efficient zero-knowledge proofs for lattice-based cryptosystems. The construction is being widely used in [1, 4].

**Lemma 1.1** ([3]). *Let $M = 2^s$ be a power-of-two. For any $i, j \in \mathbb{Z}$ satisfying $0 \leq j < i < M$, there exists $u(x) \in \mathbb{Z}[x]/\Phi_M(x)$ such that*

- $(x^i - x^j) \cdot u(x) = 2 \pmod{\Phi_M(x)}$
- *and* $||u(x)||_\infty \leq 1$.

Later, Lemma 1.1 was extended to the case of $M$ being a prime $p$ [5].

In this paper, we generalize these phenomena as the *scaled inverses* modulo cyclotomic polynomials (Definition 3.1). The scaled inverse of a nonzero element $a(x) \in \mathbb{Z}[x]/f(x)$, where $f(x)$ is an irreducible polynomial over $\mathbb{Z}$, is the element $b(x) \in \mathbb{Z}[x]/f(x)$ such that $a(x)b(x) = c \pmod{f(x)}$ for the smallest possible positive integer scale $c$. We investigate the scaled inverse of $(x^i - x^j)$ modulo cyclotomic polynomials of the form $\Phi_{p^s}(x)$ or $\Phi_{p^sq^t}(x)$.

First, we generalize the previous results [3, 5] to $\Phi_{p^s}(x)$ case: the coefficient size of the scaled inverse of $(x^i - x^j)$ is bounded by $p - 1$ with the scale $p$ modulo $\Phi_{p^s}(x)$ (Theorem 3.4). Second, we extend the results to $\Phi_{p^sq^t}(x)$ case: the coefficient size of the scaled inverse of $(x^i - x^j)$ is bounded by $q - 1$ with the scale not greater than $q$ modulo $\Phi_{p^sq^t}(x)$ (Theorem 5.3).

Our results have applications in cryptography. For instance, they are closely related to the efficiency and quality of certain zero-knowledge proofs regarding lattice-based cryptosystems with $\mathbb{Z}_{2^k}$-messages [5].[1]

Along the way of proving the theorems, we prove several properties of $\{x^k\}_{k\in\mathbb{Z}}$ in $\mathbb{Z}[x]/\Phi_{pq}(x)$ which might be of independent interest (Section 4). We also investigate so-called *expansion factors* of $\{x^k\}_{k\in\mathbb{Z}}$ in $\mathbb{Z}[x]/\Phi_{p^s}(x)$ and $\mathbb{Z}[x]/\Phi_{p^sq^t}(x)$, which also play important roles in zero-knowledge proofs regarding lattice-based cryptosystems [5]. The *expansion factor* of $f(x)$ in $\mathbb{Z}[x]/\Phi_M(x)$ is defined as the maximum value of $(||f(x) \cdot g(x)||_\infty / ||g(x)||_\infty)$ (Section 6).

## 2. Preliminaries

### 2.1. Notations

In this subsection, we list notations which we will use throughout the paper, especially the ones which might be ambiguous to some readers.

- Throughout the paper, $p, q$ are primes satisfying $p < q$, and $s, t$ are positive integers, even if they are not explicitly mentioned.
- We denote the $M$th cyclotomic polynomial as $\Phi_M(x)$ and denote the Euler's totient function as $\phi(\cdot)$, i.e., $\phi(M) = \deg \Phi_M(x)$.
- We carefully distinguish between the usage of "mod$\Phi_M(x)$"[2] and "$\pmod{\Phi_M(x)}$"[3]. We use "mod$\Phi_M(x)$" as a unary function which

[1] Utilization of $\Phi_{2^n}(x)$ cyclotomic rings gives much worse efficiency in this case.

[2] bmod in LaTeX

[3] pmod in LaTeX

reduces the input polynomial modulo $\Phi_M(x)$ so that the degree of the output is less than $\phi(M)$. On the other hand, we use "$(\mathrm{mod}\ \Phi_M(x))$" to express a certain equality holds for residue classes under $\Phi_M(x)$. For example, "$a(x) = b(x) \bmod \Phi_M(x)$" says that, when $b(x)$ is fully reduced modulo $\Phi_M(x)$, the result is exactly equal to $a(x)$ as a polynomial in $\mathbb{Z}[x]$. On the contrary, "$a(x) = b(x)\ (\mathrm{mod}\ \Phi_M(x))$" says that $a(x)$ and $b(x)$ belong to same residue class under $\Phi_M(x)$.

- We define the maximum norm $||\cdot||_\infty$ of $f(x) \in \mathbb{Z}[x]$ as the largest absolute value of coefficients of $f(x)$. We define the maximum norm $||\cdot||_\infty$ of $g(x) \in \mathbb{Z}[x]/\Phi_M(x)$ as the largest absolute value of coefficients of $(\tilde{g}(x) \bmod \Phi_M(x))$, where $\tilde{g}(x) \in \mathbb{Z}[x]$ is a representative of $g(x)$.
- For a polynomial $a(x) \in \mathbb{Z}[x]$, we denote the *reverse polynomial* of $a(x)$ as $\mathsf{rev}(a(x))$, i.e. $\mathsf{rev}(a(x)) = x^{\deg(a(x))} \cdot a(1/x)$.
- We denote the interval $\{i \in \mathbb{Z} \mid c \le i \le d\}$ as $[c, d]$.
- We denote the greatest common divisor of $a$ and $b$ as $(a, b)$.

## 2.2. Properties of cyclotomic polynomials

In this subsection, we recall and give short proofs on properties of cyclotomic polynomials $\Phi_p(x)$ and $\Phi_{pq}(x)$, which will be frequently used in the remaining parts of this paper. We only assume knowledge on basics of cyclotomic polynomials and very light knowledge on generating functions.

**Lemma 2.1.**

(a) $\Phi_{pq}(1) = 1$, *i.e.,* $\frac{\Phi_{pq}(x)-1}{x-1}$ *is a polynomial.*
(b) $\Phi_{pq}(x)$ *is symmetric, i.e.,* $\mathsf{rev}(\Phi_{pq}(x)) = \Phi_{pq}(x)$.

*Proof.* (a) Since $\Phi_p(x) \cdot \Phi_q(x) \cdot \Phi_{pq}(x) = \sum_{i=0}^{pq-1} x^i$ holds, $p \cdot q \cdot \Phi_{pq}(1) = pq$.

(b) $\Phi_{pq}(x)$ can be written as $(\sum_{i=0}^{pq-1} x^i)/(\Phi_p(x) \cdot \Phi_q(x))$. Since $\Phi_p(x) \cdot \Phi_q(x)$ is symmetric, $\Phi_{pq}(x)$ is a quotient of symmetric polynomials, where the denominator divides the divisor. □

**Lemma 2.2.** *Denote the ith coefficient of* $\frac{\Phi_{pq}(x)-1}{x-1}$ *as* $b_i$*, i.e.,* $\frac{\Phi_{pq}(x)-1}{x-1} = \sum_i b_i \cdot x^i$*. Then, we can characterize* $b_i$ *as follows.*

$$b_i = \begin{cases} 0 & \text{if } \alpha p + \beta q = i \text{ has a non-negative integer solution } (\alpha, \beta). \\ 1 & \text{otherwise.} \end{cases}$$

*Proof.* The lemma follows from the following equalities.

$$\begin{aligned} \frac{\Phi_{pq}(x)-1}{x-1} &= \frac{1}{1-x} - \frac{x^{pq}-1}{x^p-1} \cdot \frac{1}{1-x^q} \\ &= (1 + x + \cdots) - (1 + x^p + x^{2p} + \cdots + x^{pq-p})(1 + x^q + x^{2q} + \cdots). \end{aligned}$$

□

**Corollary 2.3.**

(a) *If* $p$ *divides* $i$*, the ith coefficient of* $\frac{\Phi_{pq}(x)-1}{x-1}$ *is* $0$.

(b) *For $i < q$, the $i$th coefficient of $\frac{\Phi_{pq}(x)-1}{x-1}$ is 0 if and only if $p$ divides $i$.*
(c) *For $i \geq \phi(pq)$, $\alpha \cdot p + \beta \cdot q = i$ has a non-negative integer solution $(\alpha, \beta)$.*
(d) *For $0 \leq i \leq \phi(pq) - 1$, one of the $i$th and $(\phi(pq) - i - 1)$th coefficients of $\frac{\Phi_{pq}(x)-1}{x-1}$ is 0 and the other is 1.*

*Proof.* (a) The equation $\alpha \cdot p + \beta \cdot q = t \cdot p$ has a non-negative integer solution $(t, 0)$.

(b) If $\beta$ is positive, $\alpha \cdot p + \beta \cdot q \geq q$ holds. Therefore, for $0 \leq i < q$, the equation $\alpha \cdot p + \beta \cdot q = i$ has a non-negative integer solution $(\alpha, \beta)$ if and only if $p$ divides $i$.

(c) This follows from the fact that $\deg(\frac{\Phi_{pq}(x)-1}{x-1}) = \phi(pq) - 1$.

(d) By Lemma 2.1(b), the following equalities hold. Then, recall Lemma 2.2.

$$\begin{aligned}\frac{\Phi_{pq}(x)-1}{x-1} + \mathsf{rev}\left(\frac{\Phi_{pq}(x)-1}{x-1}\right) &= \frac{\Phi_{pq}(x)-1}{x-1} + x^{\phi(pq)-1} \cdot \left(\frac{\Phi_{pq}(1/x)-1}{1/x-1}\right) \\ &= \frac{\Phi_{pq}(x)-1}{x-1} + \frac{\Phi_{pq}(x)-x^{\phi(pq)}}{1-x} \\ &= \frac{x^{\phi(pq)}-1}{x-1}.\end{aligned}$$

□

## 3. Scaled inverse of $(x^i - x^j)$ modulo $\Phi_{p^s}(x)$

In this section, we prove Theorem 3.4 regarding the scaled inverse of $(x^i - x^j)$ modulo $\Phi_{p^s}(x)$. Beforehand, we define the scaled inverse, and check its basic properties.

### 3.1. Scaled inverse

**Definition** (Scaled Inverse)**.** Let $f(x)$ be an irreducible polynomial over $\mathbb{Z}$. The scaled inverse of a nonzero element $a(x) \in \mathbb{Z}[x]/f(x)$ is the element $b(x) \in \mathbb{Z}[x]/f(x)$ such that $a(x)b(x) = c \pmod{f(x)}$ for the smallest possible positive integer $c$. We say $b(x)$ is the scaled inverse of $a(x)$ modulo $f(x)$ with scale $c$.

*Remark* 3.1 (Existence). Let $\check{a}(x) \in \mathbb{Z}[x]$ be the representative of $a(x)$ where $\deg(\check{a}) < \deg(f)$. Note that $(\check{a}(x), f(x)) = 1$, since $f(x)$ is irreducible. Thus, the resultant $r := \mathsf{res}(\check{a}(x), f(x))$ is a nonzero integer. There exist Bezout coefficients $s(x), t(x) \in \mathbb{Z}[x]$ such that $s(x)\check{a}(x) + t(x)f(x) = r$, $\deg(s) < \deg(f)$, and $\deg(t) < \deg(\check{a})$. Thus, there exists a scaled inverse with scale not greater than $r$.

*Remark* 3.2 (Uniqueness). Note the uniqueness of Bezout coefficients $\tilde{s}(x), \tilde{t}(x) \in \mathbb{Q}[x]$ such that $\tilde{s}(x)\check{a}(x) + \tilde{t}(x)f(x) = 1$, $\deg(\tilde{s}) < \deg(f)$, and $\deg(\tilde{t}) < \deg(\check{a})$. Followingly, $(c\tilde{s}(x) \bmod f(x))$ is the unique scaled inverse.

*Remark* 3.3 (Formulation). Let $\mathsf{cont}(s)$ be the positive content of $s(x)$. Let $d$ be $(r, \mathsf{cont}(s))$. Then, it is easy to see that $b(x) := s(x)/d \bmod f(x)$ is the scaled inverse with scale $c := r/d$.

### 3.2. Proof of Theorem 3.4

**Theorem 3.4.** *Let $p$ be a prime and $M = p^s$ be a prime power. For any $i, j \in \mathbb{Z}$ satisfying $0 \leq j < i < M$, there exists $u(x) \in \mathbb{Z}[x]/\Phi_M(x)$ such that*

- $(x^i - x^j) \cdot u(x) = p \pmod{\Phi_M(x)}$
- *and* $||u(x)||_\infty \leq p - 1$.

Theorem 3.4 says the coefficient size of the scaled inverse of $(x^i - x^j)$ is bounded by $p-1$ with the scale $p$ modulo $\Phi_{p^s}(x)$. Regarding Remark 3.3, $u(x)$ is indeed the scaled inverse: coefficients of $u(x)$ is already smaller than $p$, which is the only non-identity factor of $p$.

For readers' comprehension, we first review the proof of $s = 1$ case which was previously presented in [5]. The full proof of Theorem 3.4 is a straightforward generalization of the $s = 1$ case. However, the full proof requires unpleasant notations and computations. Readers might want to first read the $s = 1$ case and catch the outline of the full proof.

*Proof of Theorem 3.4.* ([5] $s = 1$ Case) Consider the following polynomial in $\mathbb{Z}[x]$.

$$v(x) := \frac{\Phi_p(x) - p}{x - 1} = \sum_{k=0}^{p-1} (p - 1 - k) \cdot x^k$$

We claim that $\tilde{u}(x) := -x^{p-j} \cdot v(x^{i-j}) \in \mathbb{Z}[x]$ satisfies the conditions after being reduced by $\Phi_p(x)$. By definition, the first condition can be easily checked with the fact that $\Phi_p(x)$ divides $\Phi_p(x^{i-j})$ since $(p, i - j) = 1$.

Since $p$ does not divide $i - j$, when reduced modulo $x^p - 1$, each monomials of $\tilde{u}(x)$ are reduced to distinct-degree monomials with coefficients remaining in the interval $[1 - p, 0]$. Let us denote the $\ell$th coefficient of $(\tilde{u}(x) \bmod x^p - 1)$ as $\tilde{u}_\ell \in [1-p, 0]$. Applying modulo $\Phi_p(x)$ to $(\tilde{u}(x) \bmod x^p - 1)$, the $\ell$th coefficients of $(\tilde{u}(x) \bmod \Phi_p(x))$ equals $\tilde{u}_\ell - \tilde{u}_{(p-1)}$. Certainly, $\tilde{u}_\ell - \tilde{u}_{(p-1)}$ lies in the interval of $[1 - p, p - 1]$. Thus, the inequality $||\tilde{u}(x) \bmod \Phi_p(x)||_\infty \leq p - 1$ holds. □

Now we give the actual proof of Theorem 3.4 for arbitrary $s$.

*Proof of Theorem 3.4.* Let $p^\alpha$ be the largest power of $p$ dividing $i - j$, and let $\beta := (i - j)/p^\alpha$. Let us denote $M' = p^{s-1}$. Consider the following polynomial $v(x) \in \mathbb{Z}[x]$.

$$\begin{aligned} v(x) &:= \frac{\Phi_M(x^\beta) - p}{x^{p^\alpha \beta} - 1} \\ &= \frac{\Phi_p(x^{M'\beta}) - p}{x^{M'\beta} - 1} \cdot \frac{x^{M'\beta} - 1}{x^{p^\alpha \beta} - 1} \\ &= \sum_{k=0}^{p-1} (p - 1 - k) \left[ x^{(M'k)\beta} + x^{(M'k + p^\alpha)\beta} + \cdots + x^{(M'k + M' - p^\alpha)\beta} \right]. \end{aligned}$$

We claim that $\tilde{u}(x) = -x^{M-j} \cdot v(x) \in \mathbb{Z}[x]$ satisfies the conditions after being reduced by $\Phi_M(x)$. By definition, the first condition can be easily checked with the fact that $\Phi_M(x)$ divides $\Phi_M(x^\beta)$ since $(M, \beta) = 1$.

For the second condition, first observe that the degrees of monomials with nonzero coefficients in $\tilde{u}(x)$ are same modulo $p^\alpha\beta$. Moreover, the coefficients of $\tilde{u}(x)$ are in the interval of $[1-p, 0]$. Since $(M, \beta) = 1$, when reduced modulo $x^M - 1$, each monomials of $\tilde{u}(x)$ are reduced to distinct-degree monomials (degrees being same modulo $p^\alpha$) with coefficients remaining in the interval of $[1-p, 0]$. Let us denote the $\ell$th coefficient of $(\tilde{u}(x) \bmod x^M - 1)$ as $\tilde{u}_\ell \in [1-p, 0]$. Applying modulo $\Phi_M(x)$ to $(\tilde{u}(x) \bmod x^M - 1)$, the $\ell$th coefficients of $(\tilde{u}(x) \bmod \Phi_M(x))$ equals $\tilde{u}_\ell - \tilde{u}_m$, where $m$ is the largest integer which equals $\ell$ modulo $M'$ and less than $M$. Certainly, $\tilde{u}_\ell - \tilde{u}_m$ lies in the interval of $[1-p, p-1]$. Thus, the inequality $||\tilde{u}(x) \bmod \Phi_M(x)||_\infty \leq p-1$ holds. □

We remark that Theorem 3.4 is tight: when $i = 1$ and $j = 0$, the 0th coefficient of $u(x)$ is $p-1$ and followingly $||u(x)||_\infty = p-1$.

## 4. Properties of $\{x^k\}_{k\in\mathbb{Z}}$ modulo $\Phi_{pq}(x)$

In this section, we prove several properties of $\{x^k\}_{k\in\mathbb{Z}}$ in $\mathbb{Z}[x]/\Phi_{pq}(x)$. These results are not only the essence of the proof of Theorem 5.1 in Section 5, but also could be of independent interest.

### 4.1. Properties of $\{x^k\}_{k\in\mathbb{Z}}$ modulo $\Phi_{pq}(x)$

**Lemma 4.1.** *The following equalities hold for* $0 \leq k \leq p-1$.

$$x^{\phi(pq)+k} \bmod \Phi_{pq}(x) = x^{\phi(pq)+k} - \Phi_{pq}(x) \cdot \sum_{i=0}^{k} x^i,$$

$$||x^{\phi(pq)+k} \bmod \Phi_{pq}(x)||_\infty = 1.$$

*Proof.* Let us denote the $j$th coefficient of $\Phi_{pq}(x) \cdot \sum_{i=0}^{k} x^i$ as $d_j$, i.e., $\Phi_{pq}(x) \cdot \sum_{i=0}^{k} x^i = \sum_j d_j \cdot x^j$. Consider the following representation.

$$\begin{aligned}\Phi_{pq}(x) \cdot \sum_{i=0}^{k} x^i &= \frac{x^{pq}-1}{(x-1)\cdot\Phi_p(x)\cdot\Phi_q(x)} \cdot \frac{x^{k+1}-1}{x-1} \\ &= \frac{x^{pq}-1}{x^p-1} \cdot \frac{1-x^{k+1}}{1-x^q} \\ &= (1+x^p+x^{2p}+\cdots+x^{(q-1)p})(1-x^{k+1})(1+x^q+x^{2q}+\cdots).\end{aligned}$$

Now we can interpret $d_i$'s combinatorially. That is, for Diophantine equations

$$\alpha p + \beta q = i, \tag{1}$$

$$\alpha p + \beta q = i - (k+1), \tag{2}$$

$$d_i = \begin{cases} 1 & \text{if (1) has a non-negative integer solution } (\alpha, \beta) \text{ but (2) does not.} \\ -1 & \text{if (2) has a non-negative integer solution } (\alpha, \beta) \text{ but (1) does not.} \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, we proved that $||x^{\phi(pq)+k} - \Phi_{pq}(x) \cdot \sum_{i=0}^{k} x^i||_\infty = 1$.

Equation (1) has a non-negative integer solution for $\phi(pq) \leq i \leq \phi(pq) + k$ (Corollary 2.3(c)). On the other hand, the equation (2) has non-negative integer solutions for any $\phi(pq) \leq i < \phi(pq) + k$ (Lemma 2.2, Corollary 2.3(b),(d)). Furthermore, it is easy to see that equation (2) has no solution for $i = \phi(pq)+k$, since $\deg(\frac{\Phi_{pq}(x)-1}{x-1}) = \phi(pq)-1$ (Lemma 2.2). Together with the combinatorial characterization of $d_i$, $d_i = 0$ holds for $\phi(pq) \leq i < \phi(pq) + k$ and $d_i = 1$ holds for $i = \phi(pq) + k$. Then, the lemma follows. □

**Corollary 4.2.** *For $0 \leq k < p-1$, the 0th coefficient of $(x^{\phi(pq)+k} \bmod \Phi_{pq}(x))$ equals $-1$.*

*Proof.* The corollary follows from Lemma 4.1 and the fact that $\Phi_{pq}(0) = 1$ by Lemma 2.1(b). □

**Corollary 4.3.** *For $0 \leq k < p-1$, the $(\phi(pq)-1)$th coefficient of $(x^{\phi(pq)+k} \bmod \Phi_{pq}(x))$ is 1.*

*Proof.* Considering the following equalities, the corollary follows from Lemma 4.1 and Corollary 2.3(b),(d).

$$\begin{aligned} \Phi_{pq}(x) \cdot \sum_{i=0}^{k} x^i &= \left( \frac{\Phi_{pq}(x) - 1}{x - 1} \cdot (x - 1) + 1 \right) \cdot \sum_{i=0}^{k} x^i \\ &= \frac{\Phi_{pq}(x) - 1}{x - 1} \cdot (x^{k+1} - 1) + \sum_{i=0}^{k} x^i. \end{aligned}$$ □

**Lemma 4.4.** *The following equality holds for $p - 1 \leq k \leq q - 1$.*

$$x^{\phi(pq)+k} \bmod \Phi_{pq}(x) = -x^{k-(p-1)} \sum_{i=0}^{p-2} x^{q \cdot i}.$$

*Proof.* The lemma directly follows from the following equalities. The first equality is from Lemma 4.1.

$$x^{\phi(pq)+p-1} \bmod \Phi_{pq}(x) = x^{pq-q} - \Phi_{pq}(x) \cdot \Phi_p(x) = x^{pq-q} - \frac{x^{pq} - 1}{x^q - 1} = -\sum_{i=0}^{p-2} x^{q \cdot i}.$$ □

**Lemma 4.5.** *The following equality holds for $0 \leq k < pq - \phi(pq)$.*

$$\mathsf{rev}\left( x^{\phi(pq)+k} \bmod \Phi_{pq}(x) \right) = x^{pq-1-k} \bmod \Phi_{pq}(x).$$

*Proof.* Let $x^{\phi(pq)+k} \bmod \Phi_{pq}(x) = x^{\phi(pq)+k} - f(x)\cdot\Phi_{pq}(x)$. Note that $\deg(f) < pq-\phi(pq)$. By the symmetry of $\Phi_{pq}(x)$ (Lemma 2.1(b)), the following equalities hold.

$$\begin{aligned}
\mathsf{rev}\left(x^{\phi(pq)+k} \bmod \Phi_{pq}(x)\right) &= \mathsf{rev}\left(x^{\phi(pq)+k} - f(x)\cdot\Phi_{pq}(x)\right)\\
&= x^{\phi(pq)-1}\left((1/x)^{\phi(pq)+k} - f(1/x)\cdot\Phi_{pq}(1/x)\right)\\
&= x^{-k-1} - \frac{f(1/x)}{x}\cdot\Phi_{pq}(x)\\
&= x^{pq}\left(x^{-k-1} - \frac{f(1/x)}{x}\cdot\Phi_{pq}(x)\right) \pmod{\Phi_{pq}(x)}\\
&= x^{pq-k-1} - \left(x^{pq-1}f(1/x)\right)\Phi_{pq}(x) \pmod{\Phi_{pq}(x)}\\
&= x^{pq-k-1} \pmod{\Phi_{pq}(x)}.
\end{aligned}$$

□

**Corollary 4.6.** *For all integer $k$, $||x^k \bmod \Phi_{pq}(x)||_\infty = 1$ holds.*

*Proof.* This follows from Lemmas 4.1, 4.4, 4.5. □

### 4.2. Reduction matrix

For a clearer demonstration, we end this section with a numerical example and how our results apply to it. Before we proceed, we define the *reduction matrix* $R_M$ of a cyclotomic polynomial $\Phi_M(x)$ as a $\phi(M) \times M$ matrix with $(i,j)$-element being the $i$th coefficient of $(x^j \bmod \Phi_M(x))$ for $0 \le i < \phi(M)$ and $0 \le j < M$.

First, it is easy to see that $R_p = (I|-\mathbf{1})$, where $-\mathbf{1}$ denotes the column filled with $-1$. For example, not writing zeroes down and denoting $+1$ and $-1$ as $+$ and $-$ respectively,

$$R_7 = \left(\begin{array}{ccccccc|c}
+ & & & & & & & - \\
 & + & & & & & & - \\
 & & + & & & & & - \\
 & & & + & & & & - \\
 & & & & + & & & - \\
 & & & & & + & & -
\end{array}\right).$$

Regarding Lemmas 4.4, 4.5, we can describe $R_{pq}$ as $(I|B_1|B_2|B_3)$, where $B_1, B_3 \in \mathbb{Z}^{\phi(pq)\times(p-1)}$ and $B_2 \in \mathbb{Z}^{\phi(pq)\times(q-p+1)}$. Lemma 4.4 says that $B_2$ is a very structured Toeplitz matrix and Lemma 4.5 says that $B_3$ is a 180° rotation of $B_1$. Corollary 4.6 says that every element of $R_{pq}$ is in $\{-1, 0, 1\}$, Corollary 4.2 says that every elements of the 0th row of $B_1$ is $-1$, and Corollary 4.3 says that every elements of the $(\phi(pq)-1)$th row of $B_1$ is 1. We can check all these

properties with $R_{3\cdot7}$ which is listed below with the same notation as $R_7$.

$$\left(\begin{array}{cccccccc|cc|cc|cc}
+ & & & & & & & & - & - & - & & & & + & + \\
 & + & & & & & & & + & & & - & & & - & \\
 & & + & & & & & & & + & & & - & & & - \\
 & & & + & & & & & - & - & & & & - & + & + \\
 & & & & + & & & & + & & & & & - & - & \\
 & & & & & + & & & & + & & & & & - & - \\
 & & & & & & + & & - & - & & & & & + & \\
 & & & & & & & + & & - & - & & & & & + \\
 & & & & & & & & + & + & & - & & & - & - \\
 & & & & & & & & & - & & & - & & + & \\
 & & & & & & & & & & - & & & - & & + \\
 & & & & & & & & + & + & & & & - & - & \\
\end{array}\right).$$

*Remark* 4.7. Let $\bar{M}$ be the largest square-free divisor of $M$ and $M' = M/\bar{M}$. Since $\Phi_M(x) = \Phi_{\bar{M}}(x^{M'})$, $R_M$ equals $R_{\bar{M}} \otimes I$, where $\otimes$ denotes the Kronecker product. In particular, $R_{p^s} = R_p \otimes I$ and $R_{p^s q^t} = R_{pq} \otimes I$ hold.

### 4.3. Patterns in reduction matrix

**Lemma 4.8.** *The following inequality holds.*

$$\sum_{i=0}^{q-1} (x^{j+ip} \bmod \Phi_{pq}(x)) = 0.$$

*Proof.*

$$\begin{aligned}
\sum_{i=0}^{q-1} (x^{j+ip} \bmod \Phi_{pq}(x)) &= x^j \cdot \sum_{i=0}^{q-1} x^{ip} \pmod{\Phi_{pq}(x)} \\
&= x^j \cdot \Phi_{pq}(x) \cdot \Phi_q(x) \pmod{\Phi_{pq}(x)} \\
&= 0 \pmod{\Phi_{pq}(x)}.
\end{aligned}$$

□

**Lemma 4.9.** *For any $0 \le k < \phi(pq)$ and $0 \le j < p$, there are at most two $i$'s in $\{0, 1, 2, \ldots, q-1\}$ such that the $k$th coefficient of $(x^{j+ip} \bmod \Phi_{pq}(x))$ is nonzero.*

*Proof.* Combining the facts that nonzero $k$th coefficients of $(x^{j+ip} \bmod \Phi_{pq}(x))$ are either $-1$ or $+1$ (Corollary 4.6) and they sum up to zero (Lemma 4.8), it is sufficient to show that there are at most three $i$'s with nonzero $k$th coefficient of $(x^{j+ip} \bmod \Phi_{pq}(x))$.

Revisiting the reduction matrix $(I|B_1|B_2|B_3)$, at most one column corresponding to one of $\{x^{j+ip}\}_i$ may lie in each of $B_1, B_3 \in \mathbb{Z}^{\phi(pq)\times(p-1)}$. In the $k$th row of the reduction matrix, $I$ has the only nonzero element at the coordinate of $(k, k)$ and $B_2$ may have nonzero element only at the coordinate of $(k, pq - q + k - q\lfloor k/q \rfloor)$ if this coordinate lies in $B_2$. However, $k \neq pq - q + k - q\lfloor k/q \rfloor \pmod{p}$ for any $0 \le k < \phi(pq)$. Hence, the lemma is proved. □

**Lemma 4.10.** *For any subset $I \subset \{0, 1, 2, \ldots, q-1\}$ and $0 \leq j < p$, the following inequality holds.*

$$\left|\left|\sum_{i \in I} \left(x^{j+ip} \bmod \Phi_{pq}(x)\right)\right|\right|_\infty \leq 1.$$

*Proof.* From Lemmas 4.8, 4.9, and Corollary 4.6, it is easy to see that the $k$th coefficients of $\{x^{j+ip} \bmod \Phi_{pq}(x)\}_{0 \leq i < q}$ are either all zero, or all zero except for one $+1$ and one $-1$. Subset-sums of these sets are in $-1, 0, 1$. □

**Corollary 4.11.** *Let $M = p^s q^t$ and $M' = M/(pq)$ be integers where $s$ and $t$ are positive integers. For any integer $0 \leq j < p$ and any family of subsets $I_k \subset \{0, 1, 2, \ldots, q-1\}$ on $0 \leq k < M'$, the following inequality holds.*

$$\left|\left|\sum_{k=0}^{M'-1} \sum_{i \in I_k} \left(x^{(j+ip)M'+k} \bmod \Phi_M(x)\right)\right|\right|_\infty \leq 1.$$

*Proof.* Since $\left(x^{(j+ip)M'+k} \bmod \Phi_M(x)\right)$ has nonzero coefficients only at the degrees those equal to $k$ modulo $M'$, terms with distinct $k$ do not interfere with each others. Therefore, it is sufficient to prove the following inequality, which can be obtained from Lemma 4.10 with $x$ substituted by $x^{M'}$:

$$\left|\left|\sum_{i \in I_k} \left(x^{(j+ip)M'} \bmod \Phi_M(x)\right)\right|\right|_\infty \leq 1.$$ □

## 5. Scaled inverse of $(x^i - x^j)$ modulo $\Phi_{p^s q^t}(x)$

In this section, we prove Theorems 5.1 and 5.3 regarding the scaled inverse of $(x^i - x^j)$ modulo $\Phi_{p^s q^t}(x)$. We begin with Theorem 5.1. Theorem 5.1 says the coefficient size of the (scaled) inverse of $(x^i - x^j)$ is bounded by $p-1$ modulo $\Phi_{p^s q^t}(x)$, if $p^s \nmid (i-j)$ and $q^t \nmid (i-j)$. The proof outline is similar to the proof of Theorem 3.4. However, the details require the results in Section 4.

**Theorem 5.1.** *Let $p$ and $q$ be primes satisfying $p < q$, and let $M = p^s q^t$ be an integer where $s$ and $t$ are positive integers. For any integers $0 \leq j < i < M$ satisfying $p^s \nmid (i-j)$ and $q^t \nmid (i-j)$, there exists $u(x) \in \mathbb{Z}[x]/\Phi_M(x)$ such that*

- $(x^i - x^j) \cdot u(x) = 1 \pmod{\Phi_M(x)}$
- *and $||u(x)||_\infty \leq p - 1$.*

*Proof.* Let $p^\alpha$ be the largest power of $p$ dividing $i-j$, let $q^\beta$ be the largest power of $q$ dividing $i-j$, and let $\gamma := (i-j)/(p^\alpha q^\beta)$. Let us denote $M' = p^{s-1} q^{t-1}$. Consider the following polynomial $v(x) \in \mathbb{Z}[x]$. Note that $\alpha \leq s-1$ and $\beta \leq t-1$ by the assumption.

$$v(x) := \frac{\Phi_M(x^\gamma) - 1}{x^{p^\alpha q^\beta \gamma} - 1} = \frac{\Phi_{pq}(x^{M'\gamma}) - 1}{x^{M'\gamma} - 1} \cdot \frac{x^{M'\gamma} - 1}{x^{p^\alpha q^\beta \gamma} - 1}.$$

We claim that $\tilde{u}(x) = -x^{M-j} \cdot v(x) \in \mathbb{Z}[x]$ satisfies the conditions after being reduced by $\Phi_M(x)$. By definition, the first condition can be easily checked by the fact that $\Phi_M(x)$ divides $\Phi_M(x^\gamma)$ since $(M, \gamma) = 1$.

For the second condition, first observe that the degrees of monomials with nonzero coefficients in $\tilde{u}(x)$ are same modulo $p^\alpha q^\beta \gamma$. Moreover, the coefficients of $\tilde{u}(x)$ are either $-1$ or 0 by Lemma 2.2. Since $(M, \gamma) = 1$, when reduced modulo $x^M - 1$, each monomials of $\tilde{u}(x)$ are reduced to distinct-degree monomials (degrees being same modulo $p^\alpha q^\beta$) with coefficients remaining in $\{-1, 0\}$.

Since there are no monomials with a degree of multiple of $pM'$ in $v(x)$ (Corollary 2.3(a)), we can group the monomials of $(\tilde{u}(x) \bmod \Phi_M(x))$ into $p-1$ classes according to the setting of Corollary 4.11. Then applying Corollary 4.11 together with the triangle inequality, we are done. □

We remark that Theorem 5.1 is *quite* tight according to the following lemma.[4]

**Lemma 5.2.** *For $u(x)$ defined in Theorem 5.1 with $i = p^{s-1}q^{t-1}(p-1)$ and $j = p^{s-1}q^{t-1}(p-2)$, the following inequality holds.*

$$||u(x)||_\infty \geq p - 2.$$

*Proof.* Using the proof of Theorem 5.1 and the following equalities, we can reduce the general case to the $M = pq$ case with $s = 1$ and $t = 1$.

$$\begin{aligned} ||u(x)||_\infty &= \left|\left| -x^{M-j} \cdot \frac{\Phi_M(x^\gamma) - 1}{x^{p^\alpha q^\beta \gamma} - 1} \bmod \Phi_M(x) \right|\right|_\infty \\ &= \left|\left| -y^{pq-(p-2)} \cdot \frac{\Phi_{pq}(y) - 1}{y - 1} \bmod \Phi_{pq}(y) \right|\right|_\infty, \quad (y = x^{p^{s-1}q^{t-1}}). \end{aligned}$$

Now consider the following polynomial in $\mathbb{Z}[x]$.

$$\tilde{u}(x) = \Phi_{pq}(x) + (p-1) \cdot \frac{\Phi_{pq}(x) - 1}{x - 1} - \sum_{i=1}^{p-1} \frac{x^{i \cdot q - p + 2} - 1}{x - 1}.$$

First, observe that $\deg(\tilde{u}) \leq \phi(pq) - 1$. Then, by the following equalities, $\tilde{u}(x)$ satisfies the first condition of Theorem 5.1 after being reduced by $\Phi_{pq}(x)$.

$$\begin{aligned} \tilde{u}(x) \cdot (x^{p-1} - x^{p-2}) &= \tilde{u}(x) \cdot x^{p-2} \cdot (x - 1) \\ &= (p-1) \cdot x^{p-2} \cdot (\Phi_{pq}(x) - 1) - \sum_{i=1}^{p-1} \left(x^{i \cdot q} - x^{p-2}\right) \\ &= -\sum_{i=1}^{p-1} x^{i \cdot q} \\ &= 1 \pmod{\Phi_{pq}(x)}. \end{aligned}$$

[4]We remark that there are $M$'s whose $u(x)$ satisfy $||u(x)||_\infty \leq p - 2$ for all $i$ and $j$ (e.g. 35). On the other hand, there are also $M$'s whose $u(x)$ satisfy $||u(x)||_\infty = p - 1$ for some $i$ and $j$ (e.g. 33).

Observe that the 0th coefficient of $\tilde{u}(x)$ equals $-(p-2)$. This easily follows from the fact that $\Phi_{pq}(0) = 1$ (Lemma 2.1(b)). Thus, $||\tilde{u}(x)||_\infty \geq p-2$. □

Theorem 5.3 is an extension of Theorem 5.1 with the help of Theorem 3.4. Theorem 5.3 says the coefficient size of the scaled inverse of $(x^i - x^j)$ is bounded by $q-1$ with the scale not greater than $q$ modulo $\Phi_{p^s q^t}(x)$. Regarding Remark 3.3 and the proof of Theorem 5.3, $u(x)$ is indeed the scaled inverse: coefficients of $u(x)$ is not divisible by the scale.

**Theorem 5.3.** *Let $p$ and $q$ be primes satisfying $p < q$, and let $M = p^s q^t$ be an integer where $s$ and $t$ are positive integers. For any integers $0 \leq j < i < M$, there exists $u(x) \in \mathbb{Z}[x]/\Phi_M(x)$ such that*

- $(x^i - x^j) \cdot u(x) = c \pmod{\Phi_M(x)}$,
- *and* $||u(x)||_\infty \leq d$,

*where* $(c, d) = \begin{cases} (q, q-1), & \text{if } p^s \mid (i-j) \\ (p, p-1), & \text{if } q^t \mid (i-j) \\ (1, p-1), & \text{otherwise.} \end{cases}$

*Proof.* If $p^s \nmid (i-j)$ and $q^t \nmid (i-j)$, use Theorem 5.1 to get $u(x)$ with $(x^i - x^j) \cdot u(x) = 1 \pmod{\Phi_M(x)}$ and $||u(x)||_\infty \leq p-1$.

If $p^s \mid (i-j)$, let $q^\beta$ be the largest power of $q$ dividing $i-j$, and let $\gamma := (i-j)/(p^s q^\beta)$. Consider the following polynomial $v(x) \in \mathbb{Z}[x]$. Note that $\beta \leq t-1$ by the assumption.

$$v(x) := \frac{\Phi_{q^t}(x^{p^s\gamma}) - q}{x^{p^s q^\beta \gamma} - 1} = \frac{\Phi_q(x^{p^s q^{t-1}\gamma}) - q}{x^{p^s q^{t-1}\gamma} - 1} \cdot \frac{x^{p^s q^{t-1}\gamma} - 1}{x^{p^s q^\beta \gamma} - 1}.$$

We claim that $\tilde{u}(x) = -x^{M-j} \cdot v(x) \in \mathbb{Z}[x]$ satisfies the conditions with $c = q$ after being reduced by $\Phi_M(x)$. By definition, the first condition can be easily checked by the fact that $\Phi_{p^s q^t}(x)$ divides $\Phi_{q^t}(x^{p^s\gamma})$ since $p^s$, $q^t$, and $\gamma$ are mutually coprime. The second condition can be shown by the same argument in the proof of Theorem 3.4.

If $q^t \mid (i-j)$, switch the role of $p$ and $q$ in the case of $p^s \mid (i-j)$. Then, we get $u(x)$ with $(x^i - x^j) \cdot u(x) = p \pmod{\Phi_M(x)}$ and $||u(x)||_\infty \leq p-1$. □

## 6. Expansion factors of $x^k$ modulo $\Phi_{p^s}(x)$ and $\Phi_{p^s q^t}(x)$

In this section, we examine so-called the *expansion factors* of $\{x^k\}_{k\in\mathbb{Z}}$ in $\mathbb{Z}[x]/\Phi_M(x)$ with $M = p^s$ or $M = p^s q^t$. The *expansion factor* of $f(x)$ in $\mathbb{Z}[x]/\Phi_M(x)$ is defined as the maximum value of $(||f(x) \cdot g(x)||_\infty / ||g(x)||_\infty)$ upon $g(x) \in \mathbb{Z}[x]/\Phi_M(x)$. The following lemmas say that the expansion factors of $\{x^k\}_{k\in\mathbb{Z}}$ modulo $\Phi_{p^s}(x)$ and $\Phi_{p^s q^t}(x)$ are not *too large*. These lemmas are generalizations of the power-of-two case: the expansion factors of $\{x^k\}_{k\in\mathbb{Z}}$ modulo $\Phi_{2^s}(x)$ are 1, since multiplying $x^k$ in $\mathbb{Z}[x]/\Phi_{2^s}(x)$ acts as *skewed*-rotation of the coefficients. The statements and proofs follow the framework of the $p$ case which is described in [5]. The results are also closely related to the quality of certain zero-knowledge proofs regarding lattice-based cryptosystems.

**Lemma 6.1.** *For $\mathcal{R} = \mathbb{Z}[x]/\Phi_{p^s}(x)$, the following equality holds.*

$$\max_{\substack{k\in\mathbb{Z}\\ g(x)\in\mathcal{R}}} \left\{ \frac{||x^k \cdot g(x)||_\infty}{||g(x)||_\infty} \right\} = 2.$$

*Proof.* Consider the reduction matrix of $\Phi_{p^s}(x)$. Since any row of the matrix has two nonzero elements and they are either $-1$ or $+1$, $||x^k \cdot g(x)||_\infty \leq 2 \cdot ||g(x)||_\infty$ holds for all $0 \leq k < p^s$. Thus, the expansion factors of $\{x^k\}_{k\in\mathbb{Z}}$ are not greater than 2.

Note that the $(p-1)$th coefficient of $x^{p-1} \cdot (-x+1) \bmod \Phi_p(x)$ is 2. Substituting $x$ with $x^{p^{s-1}}$, we can see that the expansion factor of $x^k$ in $\mathcal{R}$ with $k = (p-1) \cdot p^{s-1}$ equals 2. □

**Lemma 6.2.** *For $\mathcal{R} = \mathbb{Z}[x]/\Phi_{p^s q^t}(x)$, the following equality holds.*

$$\max_{\substack{k\in\mathbb{Z}\\ g(x)\in\mathcal{R}}} \left\{ \frac{||x^k \cdot g(x)||_\infty}{||g(x)||_\infty} \right\} = 2p.$$

*Proof.* Consider each row of the reduction matrix $R_{pq} = (I|B_1|B_2|B_3)$. The matrices $I$ and $B_2$ contain at most one nonzero element in each row. Considering the dimensions of the matrix $B_1$ and $B_3$, they contain at most $p-1$ nonzero elements in each row. In total, any row of $R_{pq}$ has at most $2p$ nonzero elements and they are either $-1$ or $+1$ (Corollary 4.6). By Remark 4.7, any row of $R_{p^s q^t}$ also has at most $2p$ nonzero elements and they are either $-1$ or $+1$. Therefore, $||x^i \cdot g(x)||_\infty \leq 2p \cdot ||g(x)||_\infty$ holds for all $i \in \mathbb{Z}$, and the expansion factors of $\{x^k\}_{k\in\mathbb{Z}}$ are not greater than $2p$.

Combining Corollaries 4.2, 4.3 and Lemma 4.4, 4.5, the $(\phi(pq)-1)$th row of $R_{pq}$ is of the form $[0,\ldots,0,+1|+1,\ldots,+1|0,\ldots,0,-1|-1,\ldots,-1]$. Thus, the $(\phi(pq)-1)$th coefficient of $x^{\phi(pq)-1} \cdot [(1 + x + \cdots + x^{p-1}) - (x^q + x^{q+1} + \cdots + x^{q+p-1})] \bmod \Phi_{pq}(x)$ is $2p$. Substituting $x$ with $x^{p^{s-1}q^{t-1}}$, we can see that the expansion factor of $x^k$ in $\mathcal{R}$ with $k = (\phi(pq)-1) \cdot p^{s-1}q^{t-1}$ equals $2p$. □

## 7. Open problems

An interesting problem is to generalize the results of this paper to ternary or even to arbitrary cyclotomic polynomials. Another direction is to investigate coefficient sizes of scaled inverses modulo cyclotomic polynomials for a wider range of polynomials than $\{x^i - x^j\}_{i,j}$. Besides $\{x^i\}$, constructing another large subset of $\mathbb{Z}[x]/\Phi_M(x)$ (i) whose elements have small expansion factors (ii) and whose differences of elements have small scaled inverses is also an interesting open problem.

## References

[1] C. Baum, D. Cozzo, and N. P. Smart, *Using topgear in overdrive: a more efficient ZKPoK for SPDZ*, inSelected areas in cryptography—SAC 2019, 274–302, Lecture Notes

in Comput. Sci., 11959, Springer, Cham, 2020. https://doi.org/10.1007/978-3-030-38471-5_12

[2] M. Beiter, *Mathematical notes*: *The midterm coefficient of the cyclotomic polynomial* $F_{pq}(x)$, Amer. Math. Monthly **71** (1964), no. 7, 769–770. https://doi.org/10.2307/2310894

[3] F. Benhamouda, J. Camenisch, S. Krenn, V. Lyubashevsky, and G. Neven, *Better zero-knowledge proofs for lattice encryption and their application to group signatures*, in Advances in cryptology—ASIACRYPT 2014. Part I, 551–572, Lecture Notes in Comput. Sci., 8873, Springer, Heidelberg, 2014. https://doi.org/10.1007/978-3-662-45611-8_29

[4] H. Chen, M. Kim, I. Razenshteyn, D. Rotaru, Y. Song, and S. Wagh, *Maliciously secure matrix multiplication with applications to private deep learning*, in Advances in cryptology—ASIACRYPT 2020. Part III, 31–59, Lecture Notes in Comput. Sci., 12493, Springer, Cham, 2020. https://doi.org/10.1007/978-3-030-64840-4_2

[5] J. H. Cheon, D. Kim, and K. Lee, *Mhz2k*: *Mpc from he over* $\mathbb{Z}_{2^k}$ *with new packing, simpler reshare, and better zkp*, Annual International Cryptology Conference, Springer, 2021, pp. 426–456.

[6] É. Fouvry, *On binary cyclotomic polynomials*, Algebra Number Theory **7** (2013), no. 5, 1207–1223. https://doi.org/10.2140/ant.2013.7.1207

[7] H. Hong, E. Lee, H. Lee, and C. Park, *Maximum gap in* (*inverse*) *cyclotomic polynomial*, J. Number Theory **132** (2012), no. 10, 2297–2315. https://doi.org/10.1016/j.jnt.2012.04.008

[8] E. Lehmer, *On the magnitude of the coefficients of the cyclotomic polynomial*, Bull. Amer. Math. Soc. **42** (1936), no. 6, 389–392. https://doi.org/10.1090/S0002-9904-1936-06309-3

[9] V. Lyubashevsky, C. Peikert, and O. Regev, *On ideal lattices and learning with errors over rings*, in Advances in cryptology—EUROCRYPT 2010, 1–23, Lecture Notes in Comput. Sci., 6110, Springer, Berlin. 2010. https://doi.org/10.1007/978-3-642-13190-5_1

[10] V. Lyubashevsky, C. Peikert, and O. Regev, *A toolkit for ring-lwe cryptography*, Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 35–54, Springer, 2013.

Jung Hee Cheon
Department of Mathematical Sciences
Seoul National University
Seoul 08826, Korea

Dongwoo Kim
Software Solutions & Algorithms Group
Western Digital Research
California 95035, USA

Duhyeong Kim
Privacy Technologies Research
Intel Labs
Oregon 97124, USA

Keewoo Lee
Department of Mathematical Sciences
Seoul National University
Seoul 08826, Korea
*Email address*: activecondor@snu.ac.kr