

# Order Formula and its Applications

Günthner

Winter 2024

## Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Proving the Order Formula</b>	<b>2</b>
2.1	Decomposition of $(\mathbb{Z}/p^k\mathbb{Z})^\times$ . . . . .	2
2.2	Applications to the formula . . . . .	3
<b>3</b>	<b>Proving the Order Formula for <math>p = 2</math></b>	<b>5</b>
3.1	Decomposition of $(\mathbb{Z}/2^k\mathbb{Z})^\times$ . . . . .	5
3.2	Discussing the remaining proof . . . . .	7
<b>4</b>	<b>The Order Formula</b>	<b>8</b>
<b>5</b>	<b>An interesting simplification</b>	<b>8</b>
<b>6</b>	<b>Applications to the perfect numbers</b>	<b>10</b>
6.1	A quick introduction . . . . .	10
6.2	The $\Xi$ -Function . . . . .	10
<b>7</b>	<b>Appendix</b>	<b>11</b>
7.1	Proof of Lemma 2.3 . . . . .	11
7.2	Proof of Lemma 2.5 . . . . .	11

## 1 Introduction

In this paper we will be examining the following order formula:

$$\frac{\text{ord}(n)}{(\mathbb{Z}/p^k\mathbb{Z})^\times} = \frac{\text{ord}(n)}{(\mathbb{Z}/p\mathbb{Z})^\times} \cdot p^{\max(0, k - k_p(n))}$$

for  $p$  an odd prime,  $k$  a natural number and  $k_p(n)$  a special function.

## 2 Proving the Order Formula

This first proof only targets  $p \neq 2$ . We will see a modified proof later which will clarify the situation for  $p = 2$ .

Before we tackle the formula directly, we should start by understanding  $(\mathbb{Z}/p^k\mathbb{Z})^\times$ .

### 2.1 Decomposition of $(\mathbb{Z}/p^k\mathbb{Z})^\times$

We know from Gauss' work that the group  $(\mathbb{Z}/p^k\mathbb{Z})^\times$  is cyclic [1], meaning that

$$(\mathbb{Z}/p^k\mathbb{Z})^\times \cong \mathbb{Z}/\varphi(p^k)\mathbb{Z}$$

with  $\varphi(p^k)$  the Euler- $\varphi$ -Function which counts the number of coprime integers smaller than the number. The value is  $\varphi(p^k) = (p-1)p^k$  and we get:

$$(\mathbb{Z}/p^k\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)p^{k-1}\mathbb{Z}$$

Next we would like to simplify  $\mathbb{Z}/(p-1)p^{k-1}\mathbb{Z}$  for which we can use the Chinese Remainder Theorem which tells us that for two coprime integers  $a, b$  we get

$$\mathbb{Z}/ab\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}$$

Now we can write

$$(\mathbb{Z}/p^k\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)p^{k-1}\mathbb{Z} \cong (\mathbb{Z}/(p-1)\mathbb{Z}) \oplus (\mathbb{Z}/p^{k-1}\mathbb{Z}) \quad (1)$$

This is still quite abstract so let's find subgroups of  $(\mathbb{Z}/p^k\mathbb{Z})^\times$  that correspond to the summands. Define the projection onto  $(\mathbb{Z}/p\mathbb{Z})^\times$ :

$$\pi_k : (\mathbb{Z}/p^k\mathbb{Z})^\times \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$$

with

$$\pi_k(n) = n \bmod p$$

One of the interesting subgroups is

$$\ker(\pi_k) = \{ n \in (\mathbb{Z}/p^k\mathbb{Z})^\times : \text{The last digit of } n \text{ is } 1 \}$$

The order of this group is  $\#\ker(\pi_k) = p^{k-1}$ . Now since equation (1)  $\ker(\pi_k)$  must lie entirely inside  $\mathbb{Z}/p^{k-1}\mathbb{Z}$ , because its order is coprime to that of  $\mathbb{Z}/(p-1)\mathbb{Z}$ . Now since

$$\#\ker(\pi_k) = \#\mathbb{Z}/p^{k-1}\mathbb{Z}$$

and one of the groups is contained in the other, the groups are equal and we can rephrase equation (1):

$$(\mathbb{Z}/p^k\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \oplus \ker(\pi_k)$$

Substituting  $(\mathbb{Z}/p\mathbb{Z})^\times$  for  $\mathbb{Z}/(p-1)\mathbb{Z}$  gives us

**Lemma 2.1.** *Decomposition of  $(\mathbb{Z}/p^k\mathbb{Z})^\times$*

$$(\mathbb{Z}/p^k\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \oplus \ker(\pi_k)$$

## 2.2 Applications to the formula

What can we learn from Lemma 2.1?

**Lemma 2.2.** *Multiplicativity of ord*

$$\text{ord}_{(\mathbb{Z}/p^k\mathbb{Z})^\times}(n) = \text{ord}_{(\mathbb{Z}/p\mathbb{Z})^\times}(n) \cdot \text{ord}_{\ker(\pi_k)}(n)$$

Which we will prove using the more general

**Lemma 2.3.** *Let  $A, B$  be arbitrary finite groups and  $(a, b) \in A \oplus B$*

$$\text{ord}_{A \oplus B}(a, b) = \text{lcm} \left( \text{ord}_A(a), \text{ord}_B(b) \right)$$

The proof of which will be deferred to the Appendix in section 7.1.

Well we know that

$$\text{ord}_{(\mathbb{Z}/p\mathbb{Z})^\times}(n) \text{ and } \text{ord}_{\ker(\pi_k)}(n) \text{ coprime}$$

since the orders of their respective groups is coprime. This simplifies the lcm to a product and proves Lemma 2.2. ( $a, b$  coprime integers implies that  $\text{lcm}(a, b) = ab$ )

Now all that remains open is  $\text{ord}_{\ker(\pi_k)}(n)$ , for this we will need the following definition:

**Definition 1.** *For  $p$  prime and  $n \in \ker(\pi_k)$ , meaning that  $n \equiv 1 \pmod{p}$*

$$k_p(n) := \max \{ i \in \mathbb{N} : n \equiv 1 \pmod{p^i} \}$$

This is almost the function from the Introduction, but with a reduced domain. Now we can prove

**Lemma 2.4.** *For  $p$  prime and  $n \in \ker(\pi_k)$*

$$\text{ord}_{\ker(\pi_k)}(n) = p^{\max(0, k - k_p(n))}$$

Let us rewrite that using  $(a)_+ := \max(0, a)$ :

$$\text{ord}_{\ker(\pi_k)}(n) = p^{\left(k - k_p(n)\right)_+}$$

In the proof of this formula we will be using

**Lemma 2.5.**  $n, l \in \mathbb{N}$ , then

$$\text{ord}_{\mathbb{Z}/l\mathbb{Z}}(n) = \frac{l}{\gcd(n, l)}$$

This lemma will again be proven in the Appendix in section 7.2.

Now this lemma only deals with the additive group  $\mathbb{Z}/p^k\mathbb{Z}$  so let us start here by proving

$$\text{ord}(t) = p^{k-k'_p(t)} \quad (2)$$

with the function  $k'_p$  the equivalent of  $k_p$  for the additive group

$$k'_p(t) := \max \{ i \in \mathbb{N} : t \equiv 0 \pmod{p^i} \}$$

To prove equation (2) we can do a simple calculation ( $\nu_p$  denotes the  $p$ -adic valuation):

$$\begin{aligned} \text{ord}(t) &\stackrel{2.5}{=} \frac{p^k}{\gcd(p^k, t)} = \frac{p^k}{p^{\min(k, \nu_p(t))}} \\ &= p^{k-\min(k, \nu_p(t))} = p^{k+\max(-k, -\nu_p(t))} \\ &= p^{\max(0, k-\nu_p(t))} = p^{\binom{k-\nu_p(t)}{+}} \end{aligned}$$

But how do we translate equation (2) to the multiplicative group and Lemma 2.4?

**Lemma 2.6.** *Given the isomorphism*

$$\begin{array}{ccc} \iota : & \mathbb{Z}/p^{k-1}\mathbb{Z} & \rightarrow \ker(\pi_k) \\ & l & \mapsto g^l \end{array}$$

and  $t \in \ker(\pi_k)$ :

$$k_p(t) = k'_p(\iota^{-1}(t))$$

*Proof.* We want to show the equality by proving that any exponent—in the set over which  $k_p$  is the maximum of—is also a valid exponent for  $k'_p$  (and vice versa)

Let  $t \in \ker(\pi_k)$  and  $i \in \mathbb{N}$  with  $t \equiv 1 \pmod{p^i}$

Now  $\iota$  restricts to an isomorphism  $\iota' : \mathbb{Z}/p^{i-1}\mathbb{Z} \rightarrow \ker(\pi_i)$ . Since neutral elements are mapped to neutral elements by isomorphisms we get

$$\iota^{-1}(t) \equiv 0 \pmod{p^{i-1}}$$

This proof also works with  $k_p$  and  $k'_p$  switched, giving us the equality. □

*Proof of Lemma 2.4.*

$$\text{ord}_{\ker(\pi_k)}(n) = \text{ord}_{\mathbb{Z}/p^{k-1}\mathbb{Z}}(\iota^{-1}(n)) \stackrel{2}{=} p^{(k-k'_p(\iota^{-1}(n)))_+} \stackrel{2.6}{=} p^{(k-k_p(n))_+}$$

□

Now we have almost proved the order formula, all that is missing is the  $k_p$  function for all natural numbers:

**Definition 2.** *Generalized  $k_p$ -function*

$$k_p(n) := \max \{ i \in \mathbb{N} : n^{\theta(n)} \equiv 1 \pmod{p^i} \} = k_p(n^{\theta(n)})$$

with

$$\theta(n) := \text{ord}_{(\mathbb{Z}/p\mathbb{Z})^\times}(\pi_k(n))$$

Now we can finish the proof of the formula by calculation:

$$\begin{aligned} \text{ord}_{(\mathbb{Z}/p^k\mathbb{Z})^\times}(n) &= \theta(n) \cdot \text{ord}_{(\mathbb{Z}/p^k\mathbb{Z})^\times}(n^{\theta(n)}) = \theta(n) \cdot p^{(k-k_p(n^{\theta(n)}))_+} \\ &= \theta(n) \cdot p^{(k-k_p(n))_+} = \text{ord}_{(\mathbb{Z}/p\mathbb{Z})^\times}(n) \cdot p^{(k-k_p(n))_+} \end{aligned}$$

### 3 Proving the Order Formula for $p = 2$

This proof really is almost the same as that in section 2, the only difference lies in the structure of  $(\mathbb{Z}/p^k\mathbb{Z})^\times$ . While  $(\mathbb{Z}/p^k\mathbb{Z})^\times$  is cyclic for  $p \neq 2$ , it is semicyclic for  $p = 2$ , it has two generators. (semicyclic for  $k \geq 3$ )

#### 3.1 Decomposition of $(\mathbb{Z}/2^k\mathbb{Z})^\times$

In this subsection  $k$  should be assumed to be at least 3.

Let us begin by finding an element of maximal order in  $(\mathbb{Z}/2^k\mathbb{Z})^\times$ :

**Lemma 3.1.**

$$\text{ord}_{(\mathbb{Z}/2^k\mathbb{Z})^\times}(3) = 2^{k-2}$$

*Proof by Induction.*

For  $k = 3$  we can do a simple computation which tells us that  $\text{ord}(3) = 2 = 2^{k-2}$ .

Now assume that  $\text{ord}(3) = 2^{k-2}$  in  $(\mathbb{Z}/2^k\mathbb{Z})^\times$ . Let us try to calculate  $3^{(2^{k-2})} \bmod 2^{k+1}$ . It is either 1 or  $2^k + 1$  as it must be  $\equiv 1 \pmod{2^k}$ . We can show that it is  $2^k + 1$  by proving

$$\nu_2(3^{(2^{k-2})} - 1) = k - 1 \quad (3)$$

If instead the value was 1 the valuation would be larger.

We will prove equation (3) by induction. For  $k = 2$  we get

$$\nu_2(3^2 - 1) = \nu_2(2) = 1 = 2 - 1$$

Now assuming that equation (3) holds for  $k$  let us compute the value for  $k + 1$ :

$$\begin{aligned} \nu_2(3^{(2^{k-1})} - 1) &= \nu_2((3^{(2^{k-2})})^2 - 1^2) \\ &= \nu_2((3^{(2^{k-2})} - 1)(3^{(2^{k-2})} + 1)) \\ &= \nu_2(3^{(2^{k-2})} - 1) + \nu_2(3^{(2^{k-2})} + 1) \\ &= k - 1 + 1 = k \text{ assuming the right addend is 1} \end{aligned}$$

Now to prove that

$$\nu_2(3^{(2^{k-2})} + 1) = 1$$

we will simply compute

$$\begin{aligned} 3^{(2^{k-2})} + 1 &\equiv (3^2)^{(2^{k-3})} + 1 \pmod{4} \\ &\equiv 1^{(2^{k-3})} + 1 \equiv 1 + 1 \equiv 2 \end{aligned}$$

□

Next we will prove

**Lemma 3.2.**  $\{-1, 3\}$  is a generating set of  $(\mathbb{Z}/2^k\mathbb{Z})^\times$

*Proof.* We know from Lemma 3.1 that

$$2 \cdot \text{ord}(3) = 2^{k-1} = \#(\mathbb{Z}/2^k\mathbb{Z})^\times$$

We also know that

$$3^l \equiv \begin{cases} 1 & \text{if } l \bmod 2 = 0 \\ 3 & \text{if } l \bmod 2 = 1 \end{cases} \pmod{8}$$

meaning that  $3^l \not\equiv -1 \pmod{2^k}$ :  $-1$  is not an element of  $\langle 3 \rangle$ , so the group  $\langle -1, 3 \rangle$  must have  $\text{ord}(-1) \cdot \text{ord}(3) = 2^{k-1}$  elements and must be equal to the entire group. □

Now we can write

$$(\mathbb{Z}/2^k\mathbb{Z})^\times \cong \langle -1 \rangle \oplus \langle 3 \rangle \quad (4)$$

However for the decomposition we would like a different form, like in Lemma 2.1. Define

$$\begin{array}{ccc} \pi_k : & (\mathbb{Z}/2^k\mathbb{Z})^\times & \rightarrow (\mathbb{Z}/4\mathbb{Z})^\times \\ & n & \mapsto n \bmod 4 \end{array}$$

**Lemma 3.3.** *Decomposition of  $(\mathbb{Z}/2^k\mathbb{Z})^\times$  (for  $k \geq 3$ )*

$$(\mathbb{Z}/2^k\mathbb{Z})^\times \cong (\mathbb{Z}/4\mathbb{Z})^\times \oplus \ker(\pi_k)$$

*Proof.*

$$(\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \cong \langle -1 \rangle$$

For  $\ker(\pi_k)$  we will show that  $\langle -3 \rangle \triangleleft \ker(\pi_k)$  and  $\# \langle -3 \rangle = \# \ker(\pi_k)$ :

$$\pi_k(-3) \equiv -1 \cdot 3 \equiv -1 \cdot -1 \equiv 1 \pmod{4}$$

Now also all powers of  $-3$  will be in the kernel.

$$\begin{aligned} \# \langle -3 \rangle &= \text{ord}(-3) = \text{lcm}(\text{ord}(-1), \text{ord}(3)) \\ &= 2^{k-2} = \# \ker(\pi_k) \end{aligned}$$

□

### 3.2 Discussing the remaining proof

The proof that remains is entirely equivalent to the one from section 2, so only an outline of the revised version will be given.

Lemma 3.3 together with Lemma 2.3 gives us the following formula:

$$\text{ord}_{(\mathbb{Z}/2^k\mathbb{Z})^\times}(n) = \text{lcm} \left( \text{ord}_{(\mathbb{Z}/4\mathbb{Z})^\times}(n), \text{ord}_{\ker(\pi_k)}(n) \right) \quad (5)$$

This does not—unlike Lemma 2.2—simplify into a product.

Now all steps until Definition 2 will translate naturally (not in the category-theoretic sense). In the definition of  $k_2$  we must replace  $\theta$ :

**Definition 3.** *Generalized  $k_2$ -function*

$$k_p(n) := \max \{ i \in \mathbb{N} : n^{\theta(n)} \equiv 1 \pmod{p^i} \} = k_p(n^{\theta(n)})$$

with

$$\theta(n) := \text{ord}_{(\mathbb{Z}/4\mathbb{Z})^\times}(\pi_k(n))$$

The last step that may be difficult to simply believe is the final calculation:

$$\begin{aligned} \text{ord}_{(\mathbb{Z}/2^k\mathbb{Z})^\times}(n) &\stackrel{5}{=} \text{lcm} \left( \text{ord}_{(\mathbb{Z}/4\mathbb{Z})^\times}(n), \text{ord}_{\ker(\pi_k)}(n) \right) \\ &\stackrel{2.4}{=} \text{lcm} \left( \text{ord}_{(\mathbb{Z}/4\mathbb{Z})^\times}(n), 2^{\binom{k-k_2(n)}{+}} \right) \end{aligned}$$

Now we have proved the order formula for  $k \geq 3$ , but the reader may verify that the formula is also valid for  $k = 2$ . Now we can formulate the main result of this paper:

## 4 The Order Formula

**Theorem 1** (The Order Formula). *For  $p$  prime and  $k, n \in \mathbb{N}$  the following equation holds:*

$$\text{ord}_{(\mathbb{Z}/p^k\mathbb{Z})^\times}(n) = \begin{cases} \theta_p(n) \cdot p^{\binom{k-k_p(n)}{+}} & \text{if } p \neq 2 \\ \text{lcm}(\alpha_k \cdot \theta_p(n), 2^{\binom{k-k_2(n)}{+}}) & \text{if } p = 2 \end{cases}$$

with

$$\theta_p(n) = \begin{cases} \text{ord}_{(\mathbb{Z}/p\mathbb{Z})^\times}(n) & \text{if } p \neq 2 \\ \text{ord}_{(\mathbb{Z}/4\mathbb{Z})^\times}(n) & \text{if } p = 2 \end{cases}$$

and

$$k_p(n) := \max \{ i \in \mathbb{N} : n^{\theta_p(n)} \equiv 1 \pmod{p^i} \}$$

further

$$\alpha_k = \begin{cases} 1 & \text{if } k \neq 1 \\ \frac{1}{2} & \text{if } k = 1 \end{cases}$$

## 5 An interesting simplification

In this section we will try to simplify the following expression (which will be relevant for perfect numbers):

$$\nu_p(q^{\nu_q(n)+1} - 1)$$

with  $q \neq p$  prime and  $n \in \mathbb{N}$ . Let  $k$  equal the expression. Then we know that  $q^{\nu_q(n)+1} \equiv 1 \pmod{p^k}$ . We can actually write  $k$  as the maximum of all  $k$  with this property:

$$\nu_p(q^{\nu_q(n)+1} - 1) = \max \{ k \in \mathbb{N} : q^{\nu_q(n)+1} \equiv 1 \pmod{p^k} \}$$



Why? Because the condition must hold for all smaller  $k$  and also the actual  $k$  (the expression) must be at least as large as any of the admissible  $k$ .

Now let us rewrite the admissibility condition (for now assume  $p \neq 2$ ):

$$\begin{aligned} q^{\nu_q(n)+1} \equiv 1 \pmod{p^k} &\iff \text{ord}(q) \mid \nu_q(n) + 1 \\ &\iff \theta_p(n) \cdot p^{\binom{k-k_p(n)}{+}} \mid \nu_q(n) + 1 \\ &\iff \theta_p(n) \mid \nu_q(n) + 1 \wedge p^{\binom{k-k_p(n)}{+}} \mid \nu_q(n) + 1 \end{aligned}$$

Let us continue with the right side of the  $\wedge$ :

$$\begin{aligned} p^{\binom{k-k_p(n)}{+}} \mid \nu_q(n) + 1 &\iff (k - k_p(n))_+ \leq \nu_p(\nu_q(n) + 1) \\ &\iff k - k_p(n) \leq \nu_p(\nu_q(n) + 1) \end{aligned}$$

Now if  $\theta_p(n) \nmid \nu_q(n) + 1$  we get

$$\nu_p(q^{\nu_q(n)+1} - 1) = 0$$

as this is the only  $k$  where The Order Formula does not apply. Now assuming that  $\theta_p(n) \mid \nu_q(n) + 1$ :

$$\nu_p(q^{\nu_q(n)+1} - 1) = k_p(n) + \nu_p(\nu_q(n) + 1)$$

as this is the last  $k$  such that the inequality holds.

Let's rewrite the condition for  $p = 2$ :

$$\begin{aligned} q^{\nu_q(n)+1} \equiv 1 \pmod{p^k} &\iff \text{ord}(q) \mid \nu_q(n) + 1 \\ &\iff \text{lcm}\left(\alpha_k \cdot \theta_p(n), 2^{\binom{k-k_2(n)}{+}}\right) \mid \nu_q(n) + 1 \\ &\iff \alpha_k \cdot \theta_p(n) \mid \nu_q(n) + 1 \wedge 2^{\binom{k-k_2(n)}{+}} \mid \nu_q(n) + 1 \end{aligned}$$

Again continuing with the right side of the  $\wedge$ :

$$2^{\binom{k-k_2(n)}{+}} \mid \nu_q(n) + 1 \iff k - k_2(n) \leq \nu_2(\nu_q(n) + 1)$$

If  $\theta_2(n) \nmid \nu_q(n) + 1$ , then

$$\nu_2(q^{\nu_q(n)+1} - 1) = 1$$

as  $q$  is odd. If instead  $\theta_2(n) \mid \nu_q(n) + 1$ :

$$\nu_2(q^{\nu_q(n)+1} - 1) = k_2(n) + \nu_2(\nu_q(n) + 1)$$

Now for the result of this section:

**Lemma 5.1.** *Let  $p \neq q$  prime and  $n \in \mathbb{N}$*

$$\nu_p(q^{\nu_q(n)+1} - 1) = \begin{cases} k_p(n) + \nu_p(\nu_q(n) + 1) & \text{if } \theta_p(n) \mid \nu_q(n) + 1 \\ \delta_{p,2} & \text{if } \theta_p(n) \nmid \nu_q(n) + 1 \end{cases}$$

## 6 Applications to the perfect numbers

### 6.1 A quick introduction

**Definition 4.**

$$\sigma_t(n) = \sum_{x|n} x^t$$

**Lemma 6.1.** *For  $t \neq 0$*

$$\sigma_t(n) = \prod_{p \text{ prime}} \frac{p^{(\nu_p(n)+1)t} - 1}{p^t - 1}$$

This is a result from [2].

**Definition 5.** *Perfect number.*

$$n \text{ is perfect iff } 2n = \sigma_1(n)$$

### 6.2 The $\Xi$ -Function

**Definition 6.** *The  $\Xi$ -Function:*

$$\Xi_n(q, p) := \begin{cases} k_p(n) + \nu_p(\nu_q(n) + 1) - \nu_p(q - 1) & \text{if } \theta_p(n) \mid \nu_q(n) + 1 \\ \delta_{p,2} & \text{if } \theta_p(n) \nmid \nu_q(n) + 1 \end{cases}$$

There is an implicit  $-\nu_p(q - 1)$  in the lower case, which is however zero if  $\theta_p(n) \nmid \nu_q(n) + 1$ . Now we get

$$\Xi_n(q, p) = \nu_p \left( \frac{p^{\nu_q(n)+1} - 1}{q - 1} \right)$$

which relates it to  $\sigma_1$ :

$$\begin{aligned} \nu_p(\sigma_1(n)) &= \nu_p \left( \prod_{q \text{ prime}} \frac{q^{\nu_q(n)+1} - 1}{q - 1} \right) \\ &= \sum_{q \text{ prime}} \nu_p \left( \frac{q^{\nu_q(n)+1} - 1}{q - 1} \right) \\ &= \sum_{q \text{ prime}} \Xi_n(q, p) \end{aligned}$$

## 7 Appendix

### 7.1 Proof of Lemma 2.3

**Lemma 2.3.** *Let  $A, B$  be arbitrary finite groups and  $(a, b) \in A \oplus B$*

$$\text{ord}_{A \oplus B}(a, b) = \text{lcm} \left( \text{ord}_A(a), \text{ord}_B(b) \right)$$

*Proof.*

Let  $o_a, o_b$  denote  $\text{ord}(a), \text{ord}(b)$  respectively and let  $o_{ab}$  denote  $\text{ord}(a, b)$ .

$o_a \mid o_{ab}$ , since  $n^{o_a} = e$  (Same for  $o_b$ ). This gives us  $\text{lcm}(o_a, o_b) \mid o_{ab}$ .

$o_{ab} \mid \text{lcm}(o_a, o_b)$ , since  $(a, b)^{\text{lcm}(o_a, o_b)} = (a^{\text{lcm}(o_a, o_b)}, b^{\text{lcm}(o_a, o_b)}) = (e, e)$

□

### 7.2 Proof of Lemma 2.5

**Lemma 2.5.**  *$n, l \in \mathbb{N}$ , then*

$$\text{ord}_{\mathbb{Z}/l\mathbb{Z}}(n) = \frac{l}{\gcd(n, l)}$$

*Proof.* A number  $x$  is equal to  $\text{ord}(n)$  exactly if it is the smallest number such that  $l \mid nx$ . Now  $n \cdot \text{ord}(n) = \text{lcm}(n, l)$ . The smallest multiple of  $n$  that is divisible by  $l$ . Now calculate

$$n \cdot \frac{l}{\gcd(n, l)} = \frac{nl}{\gcd(n, l)} = \text{lcm}(n, l)$$

telling us that  $\frac{l}{\gcd(n, l)} = \text{ord}(n)$

□

## References

- [1] Carl Gauss. *Disquisitiones Arithmeticae*.
- [2] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. 6th. Revised by D. R. Heath-Brown and J. H. Silverman. Foreword by Andrew Wiles. Originally published in 1938. Oxford University Press, 2008. ISBN: 978-0-19-921986-5.