

Order Formula and its Applications

Günthner

Winter 2024

Contents

1	Introduction	1
2	Proving the Order Formula	1
2.1	Decomposition of $(\mathbb{Z}/p^k\mathbb{Z})^\times$	2
2.2	Applications to the formula	3
3	Proving the Order Formula for $p = 2$	5
4	Appendix	5
4.1	Proof of Lemma 3	5
4.2	Proof of Lemma 5	6

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 and 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- φ -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 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 1?

Lemma 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 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 4.1.

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. (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 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 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 4.2.

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 (ν_p denotes the p -adic valuation):

$$\begin{aligned} \text{ord}(t) &\stackrel{5}{=} \frac{p^k}{\gcd(p^k, t)} = \frac{p^k}{p^{\min(k, \nu_p(t))}} \\ &= p^{k-\min(k, \nu_p(t))} = p^{k+\max(-k, -\nu_p(t))} \\ &= p^{\max(0, k-\nu_p(t))} = p^{\binom{k-\nu_p(t)}{+}} \end{aligned}$$

But how do we translate equation (2) to the multiplicative group and Lemma 4?

Lemma 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 ι 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 4.

$$\text{ord}_{\ker(\pi_k)}(n) = \text{ord}_{\mathbb{Z}/p^{k-1}\mathbb{Z}}(\iota^{-1}(n)) \stackrel{2}{=} p^{\binom{k-k'_p(\iota^{-1}(n))}{+}} \stackrel{6}{=} p^{\binom{k-k_p(n)}{+}}$$

□

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:

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

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 $k \geq 3$)

4 Appendix

4.1 Proof of Lemma 3

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

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

□

4.2 Proof of Lemma 5

Lemma 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*.