Order Formula and its Applications

Günthner

Winter 2024

Contents

1 Introduction

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

$$\underset{\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times}{\operatorname{ord}}(n) = \underset{\left(\mathbb{Z}/p\mathbb{Z}\right)^\times}{\operatorname{ord}}(n) \cdot p^{\max(0, k - k_p(n))}$$

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 $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$.

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

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

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

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:

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

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

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

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

$$\pi_k : \left(\mathbb{Z}/p^k\mathbb{Z}\right)^{\times} \to (\mathbb{Z}/p\mathbb{Z})^{\times}$$

with

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

One of the interesting subgroups is

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

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):

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

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

Lemma 1. *Decomposition of* $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^{\times}$

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

2.2 Applications to the formula

What can we learn from Lemma 1?

Lemma 2. *Multiplicativity of* ord

$$\underset{\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times}{\operatorname{ord}}(n) = \underset{(\mathbb{Z}/p\mathbb{Z})^\times}{\operatorname{ord}}(n) \cdot \underset{\ker(\pi_k)}{\operatorname{ord}}(n)$$

Which we will prove using the more general

Lemma 3. *Let A, B be arbitrary finite groups and* $(a, b) \in A \oplus B$

$$\underset{A\oplus B}{\operatorname{ord}}(a, b) = \operatorname{lcm}\left(\underset{A}{\operatorname{ord}}(a),\ \underset{B}{\operatorname{ord}}(b)\right)$$

The proof of which will be deferred to the Appendix in section 3.1.

Well we know that

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

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 $\operatorname{lcm}(a, b) = ab$)

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

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

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

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

Lemma 4. *For p prime and* $n \in \ker(\pi_k)$

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

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

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

In the proof of this formula we will be using

Lemma 5. *$n, l \in \mathbb{N}$, then*

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

This lemma will again be proven in the Appendix in section 3.2.
Now this lemma only deals with the additive group $\mathbb{Z}/p^k\mathbb{Z}$ so let us start here by proving

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

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):

$$\begin{aligned}\operatorname{ord}(t) &\overset{5}{=} \frac{p^k}{\gcd(p^k, t)} = \frac{p^k}{p^{\min(k,\nu_p(t))}} \\ &= p^{k-\min(k,\nu_p(t))} = p^{k+\max(-k,-\nu_p(t))} \\ &= p^{\max(0,k-\nu_p(t))} = p^{\left(k-\nu_p(t)\right)_+}\end{aligned}$$

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

Lemma 6. *Given the isomorphism*

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

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 $\iota' : \mathbb{Z}/p^{i-1}\mathbb{Z} \to \ker(\pi_i)$. 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. $\square$

Proof of Lemma 4.

$$\underset{\ker(\pi_k)}{\operatorname{ord}}(n) = \underset{\mathbb{Z}/p^{k-1}\mathbb{Z}}{\operatorname{ord}}(\iota^{-1}(n)) \overset{2}{=} p^{k-k'_p(\iota^{-1}(n))} \overset{6}{=} p^{k-k_p(n)}$$

$\square$

3 Appendix

3.1 Proof of Lemma 3

Lemma 3. *Let A, B be arbitrary finite groups and $(a, b) \in A \oplus B$*

$$\operatorname*{ord}_{A\oplus B}(a,b) = \operatorname{lcm}\left(\operatorname*{ord}_{A}(a),\ \operatorname*{ord}_{B}(b)\right)$$

Proof.
Let o_a, o_b denote $\operatorname*{ord}_{A}(a), \operatorname*{ord}_{B}(b)$ respectively and let o_{ab} denote $\operatorname*{ord}_{A\oplus B}(a,b)$.
$o_a \mid o_{ab}$, since $n^{o_{ab}} = e$ (Same for o_b). This gives us $\operatorname{lcm}(o_a, o_b) \mid o_{ab}$.
$o_{ab} \mid \operatorname{lcm}(o_a, o_b)$, since $(a,b)^{\operatorname{lcm}(o_a,o_b)} = (a^{\operatorname{lcm}(o_a,o_b)}, b^{\operatorname{lcm}(o_a,o_b)}) = (e, e)$

□

3.2 Proof of Lemma 5

Lemma 5. *$n, l \in \mathbb{N}$, then*

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

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

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

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

References

[1] Carl Gauss. *Disquisitiones Arithmeticae.*