Order Formula and its Applications

Günthner

Winter 2024

1 Introduction

In this paper we will be examining the following formula:

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

2 Proving the Order Formula

2.1 Examining Simpler Groups

We would like to simply the order in one of the multiplicative groups by recursively examining smaller and smaller subgroups. For this we should first find a recursion formula for the order in groups depending on that in a smaller group.

Let p be prime, $k \in \mathbb{N}$. Now let $n \in \mathbb{Z}/p^{k+1}\mathbb{Z}$ be an arbitrary element, we are interested in the following value:

$$\frac{\mathrm{ord}_{\mathbb{Z}/p^{k+1}\mathbb{Z}}(n)}{\mathrm{ord}_{\mathbb{Z}/p^k\mathbb{Z}}(n \bmod p^k)} \tag{1}$$

the change of the order.

First we shall simplify the order in the quite simple group $\mathbb{Z}/x\mathbb{Z}$:

Lemma 1.

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

Proof. We would like to show that for $t \in \mathbb{N}$

$$t \cdot l \equiv 0 \pmod x \iff x \mid tl \iff \frac{x}{\gcd(x, l)} \mid t$$

Assume that $\frac{x}{\gcd(x,l)} \mid t$, meaning that $t = \frac{x}{\gcd(x,l)} \cdot \square$ with $\square$ denoting an unimportant value. Let us examine

$$\frac{x \cdot l}{\gcd(x, l)} = \mathrm{lcm}(x, l) \equiv 0 \pmod x$$

Now assume instead that $x \mid tl$:

$$\frac{x}{\gcd(x,l)} \gcd(x,l) \mid tl$$

But since already $\gcd(x,l) \mid l$ and also $\frac{x}{\gcd(x,l)}$ and l are coprime, it must be that

$$\frac{x}{\gcd(x,l)} \mid t$$

□

Using Lemma 1 we find the following formula:

$$\begin{aligned}\operatorname{ord}_{\mathbb{Z}/p^k\mathbb{Z}}(n) &= \frac{p^k}{\gcd(p^k,n)} = p^{k-\min(k,\nu_p(n))} \\ &= p^{k+\max(-k,-\nu_p(n))} = p^{\max(0,k-\nu_p(n))}\end{aligned}$$

Now let us apply that to equation (1):

$$\begin{aligned}\frac{\operatorname{ord}_{\mathbb{Z}/p^{k+1}\mathbb{Z}}(n)}{\operatorname{ord}_{\mathbb{Z}/p^k\mathbb{Z}}(n \bmod p^k)} &= \frac{p^{\max(0,k+1-\nu_p(n))}}{p^{\max(0,k-\nu_p(n \bmod p^k))}} \\ &= p^{\max(0,k+1-\nu_p(n))-\max(0,k-\nu_p(n \bmod p^k))} \\ &=: p^{\mathfrak{c}}\end{aligned}$$

If we write $n =: m + rp^k$, $m < p^k$, $r < p$ and $\max(0,x) =: x_+$ we can rewrite the formula for $\mathfrak{c}$ like so:

$$\begin{aligned}\mathfrak{c} &= \max(0,k+1-\nu_p(n)) - \max(0,k-\nu_p(n \bmod p^k)) \\ &= \Big(k+1-\nu_p(m+rp^k)\Big)_+ - \Big(k-\nu_p(m)\Big)_+\end{aligned}$$

For the values of $\mathfrak{c}$ we find the following table:

	$r = 0$	$r \neq 0$
$m = 0$	0	1
$m \neq 0$	1	1

Proof for $m = 0$ and $r = 0$.

$$\begin{aligned}\mathfrak{c} &= \Big(k+1-\nu_p(0+0)\Big)_+ - \Big(k-\nu_p(0)\Big)_+ \\ &= \Big(k+1-\infty\Big)_+ - \Big(k-\infty\Big)_+ = 0 - 0 = 0\end{aligned}$$

□

Proof for $m = 0$ and $r \neq 0$.

$$\begin{aligned}\mathfrak{c} &= \Big(k + 1 - \nu_p(rp^k)\Big)_+ - \Big(k - \nu_p(m)\Big)_+ \\ &= \Big(k + 1 - k\Big)_+ - 0 = 1\end{aligned}$$

□

Proof for $m \neq 0$.

$$\begin{aligned}\mathfrak{c} &= \Big(k + 1 - \nu_p(m + rp^k)\Big)_+ - \Big(k - \nu_p(m)\Big)_+ \\ &= \Big(k + 1 - \nu_p(m)\Big)_+ - \Big(k - \nu_p(m)\Big)_+ \\ &= \Big(k + 1 - \nu_p(m)\Big) - \Big(k - \nu_p(m)\Big) = 1\end{aligned}$$

Here we are using that

$$\nu_p(a) < \nu_p(b) \implies \nu_p(a + b) = \nu_p(a)$$

and that

$$0 < a < p^k \implies \nu_p(a) < k$$

□