Die Anzahl an Orbits unter Multiplikation modulo eine Zahl

Jonathan Günthner

Sommer 2024

1 Abstract

Worum geht es hier kurz und knapp? Wie viele Zyklen gibt es, wenn man immer wieder mit einer Zahl multipliziert und das Ergebnis dann modulo eine andere Zahl nimmt.

Das Ergebnis dieses Papers ist, dass für $m, n \in \mathbb{P}$ mit $\gcd(m, n)$ die Anzahl an Zyklen/Orbits modulo n

$$\sum_{e_0=0}^{v_2(n)} \sum_{e_1=0}^{v_{p_1}(n)} \sum_{e_2=0}^{v_{p_2}(n)} \cdots \sum_{e_\square=0}^{v_{p_\square}(n)} \frac{\prod\limits_{i\in\mathbb{N}} \phi(p_i^{e_i})}{\operatorname{lcm}\{\operatorname{ord}_{(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*}(m) \mid i \in \mathbb{N}_0\}}$$

ist.

Weiterhin werde ich zeigen, dass für $p \in \mathbb{P} \setminus \{2\}$ und $m \in \mathbb{N} \setminus p\mathbb{N}$ und $k \in \mathbb{N}$

$$\operatorname{ord}_{(\mathbb{Z}/p^k\mathbb{Z})^*}(m) = \operatorname{ord}_{(\mathbb{Z}/p\mathbb{Z})^*}(m) \cdot p^{\max\{0, k-k_0+1\}}$$

Letztlich möchte ich noch eine algorithmische Implementierung der letzten Gleichung präsentieren, die die Ordnung für bestimmte Zahlen sehr schnell berechnen kann.

2 Grundlagen

Diesen Teil kann man getrost überspringen, wenn man die Euler-ϕ-Funktion, die Primfaktorzerlegung, die p-adische Werigkeit, Modulorechnen, Äquivalenzklassen, abelsche Gruppen, Lagranges Satz, Homo- und Isomorphismen, die Direkte Summe und den Fundamentalsatz der abelschen Gruppen gut verstranden hat.

Hier eine Übersicht zu der Einführung:

- Die Primfaktorzerlegung
- Die p-adische Wertigkeit
- Die Funktionen gcd und lcm
- Die Euler-ϕ-Funktion
- Restklassen
- (abelsche) Gruppen
- Ein kurzer Abstecher zu Ringen
- Homomorphismen auf Gruppen
- Primitive Elemente auf Gruppen
- Die Ordnung und der Satz von Lagrange
- Die Direkte Summe und der Fundamentalsatz der abelschen Gruppen

2.1 Primfaktorzerlegung

Jede natürliche Zahl n kann man auf eine und nur eine Art und Weise als Produkt von Primpotenzen schreiben. Zum Beispiel

$$12 = 2^2 \cdot 3$$

Hier beachten wir also nicht die Reihenfolge.

Das sieht dann ganz allgemein dann so aus:

$$n = p_1^{v_1} \cdot p_2^{v_2} \cdot \ldots$$

Eine Primzahl $p \in \mathbb{P}$ hat immer den Exponenten $v \in \mathbb{N}$ in der Primfaktorzerlegung, wie oft man n durch p teilen kann.

2.2 p-adische Wertigkeit

Die p-adische Wertigkeit v_p einer Zahl n ist, wie oft man z durch p teilen kann. Das ist ist das gleiche, wie der Exponent in dem vorherigen Abschnitt. Somit gilt für $n \in \mathbb{N}$:

$$n = \prod_{p \in \mathbb{P}} p^{v_p(x)}$$

Also jede Primzahl taucht genauso oft in der Zerlegung auf, wie die Zahl durch die Primzahl teilbar ist.

Für v_p gelten ein paar Rechenregeln:

Lemma 2.1. *Für alle $a, b \in Z$ und $p \in \mathbb{P}$*

$$v_p(a \cdot b) = v_p(a) + v_p(b)$$

Wenn man a $v_p(a)$-Mal durch p teilen kann und b $v_p(b)$-Mal durch p teilen kann, dann kann man $a \cdot b$ $v_p(a)$-Mal und dann noch mal $v_p(b)$-Mal durch p teilen.

Lemma 2.2. *Für alle $a, b \in \mathbb{Z}$ und $p \in \mathbb{P}$*

$$v_p(a+b) = \begin{cases} v_p(a) & & v_p(a) < v_p(b) & \\ v_p(b) & \textit{falls} & v_p(a) > v_p(b) & \\ v_p(a) & & v_p(a) = v_p(b) & \wedge\, p^{v_p(a)+1} \nmid a+b \\ > v_p(a) & & v_p(a) = v_p(b) & \wedge\, p^{v_p(a)+1} \mid a+b \end{cases}$$

Die Hauptaussage hier ist praktisch, dass, wenn in einer Summe die Wertigkeiten der einzelnen Zahlen unterschiedlich sind, dann die Wertigkeit der Summe das Minimum beider Wertigkeiten ist.

Beweis. Nehmen wir $n, t \in \mathbb{N}$ und $p \in \mathbb{P}$ mit $v_p(t) > 0$

Nun gilt

$$v_p(n) < v_p(tn) = v_p(n) + v_p(t)$$

Wenn wir nun $tn + n$ betrachten, dann

$$tn + n = n(t+1)$$

aber entweder $p \mid t$ oder $p \mid t+1$ und da $p \mid t$

$$v_p(t+1) = 0$$

und

$$v_p(n(t+1)) = v_p(n) + v_p(t+1) = v_p(n)$$

□

Die unteren beiden Fälle- möchte ich hier nicht erörtern, aber man versteht sie am besten, in dem man sich die Addition zweier Zahl in der Basis p anschaut.

2.3 gcd und lcm

Definition 2.3. *Für $a, b \in \mathbb{N}$ ist $\gcd(a, b)$ die größte natürliche Zahl, die a und b teilt. (**G**reatest **C**ommon **D**ivisor)*

Definition 2.4. $\operatorname{lcm}(a, b)$ *ist die kleinste natürliche Zahl, die sowohl ein Vielfaches von a und auch von b ist. (**L**east **C**ommon **M**ultiple)*

Definition 2.5. *Coprim*

Zwei Zahlen $a, b \in \mathbb{N}$ sind coprim, wenn es keine natürliche Zahl $n \neq 1$ gibt mit $n \mid a$ und $n \mid b$.

Wenn zwei Zahlen $a, b \in \mathbb{N}$ coprim sind, genau dann gilt $\gcd(a, b) = 1$.

Lemma 2.6. *Seien $a, b, c \in \mathbb{N}$ mit a und b coprim, also $\gcd(a, b) = 1$*

$$\gcd(ab, c) = \gcd(a, c) \cdot \gcd(b, c)$$

Lemma 2.7. *Seien $a, b, c \in \mathbb{N}$ mit a und b coprim*

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

2.4 Euler-ϕ-Funktion

Definition 2.8. *Für $n \in \mathbb{N}$ ist $\phi(n)$ die Anzahl an natürlichen Zahlen k mit $k < n$ und k und n coprim.*

Lemma 2.9. *Für alle $p \in \mathbb{P}$*

$$\phi(p) = p - 1$$

Also alle natürlichen Zahlen, die kleiner als p sind, haben keine gemeinsamen Faktoren mit p, was auch Sinn ergibt, da p ansonsten nicht prim wäre.

Lemma 2.10. *Für alle $a, b \in \mathbb{N}$ mit a und b coprim*

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$$

Beispiel 2.11. *$a = 2$ und $b = 3$*

Nur 1 ist coprim zu 2 somit $\phi(2) = 1$

Nur 1 und 2 sind coprim zu 3 somit $\phi(3) = 2$

Nun erwarten wir $\phi(6) = \phi(2) \cdot \phi(3) = 1 \cdot 2 = 2$.

Es sind nur 1 und 5 coprim zu 6, somit ist tatsächlich $\phi(6) = 2$

Lemma 2.12. *Für alle $n \in \mathbb{N}$ und $p \in \mathbb{P}$*

$$\phi(p^n) = \phi(p) \cdot p^{n-1} = (p - 1) \cdot p^{n-1}$$

Beispiel 2.13. *$p = 3$ und $n = 2$*

$\phi(3) = 2$ und wir erwarten nun, dass $\phi(9) = \phi(3) \cdot 3^1 = 6$.

Nur $1, 2, 4, 5, 7, 8$ sind coprim zu 6 womit die Aussage hier stimmt.

2.5 Restklassen

Was ist das also? Betrachten wir ein Beispiel.

Beispiel 2.14. *Wir wollen wissen, ob*

$$\forall n \in \mathbb{N} : n^2 + n + 1 \textit{ gerade}$$

Dafür, würde ich behaupten, müssen wir wissen, ob n^2 gerade ist.

Lemma 2.15.

$$n \textit{ gerade} \iff n^2 \textit{ gerade}$$

Beweis.
Falls n gerade, also $n = 2k$ für ein $k \in \mathbb{N}$, dann

$$n^2 = (2k)^2 = 2 \cdot (2 \cdot k^2)$$

somit n^2 gerade
Falls $\neg(n$ gerade), also $n = 2k - 1$ für ein $k \in \mathbb{N}$, dann

$$\begin{aligned} n^2 &= (2k-1)^2 \\ &= (2k)^2 - 2(2k \cdot 1) + 1 \\ &= 2(2k^2) - 2(2k \cdot 1) + 1 \\ &= 2(2k^2 - k \cdot 1) + 1 \end{aligned}$$

Also ist n^2 eine gerade Zahl plus 1 und somit ungerade.

□

Lemma 2.16. *Das geht auch viel einfacher*

Ich würde postulieren, dass alles, was entscheidet, ob ein Ausdruck wie $n^2 + n + 1$ gerade ist, folgendes ist: ob die Bestandteile gerade sind.

Schreiben wir nun also $n \equiv 2 \pmod 2$, wenn die Zahl n gerade ist, um auszudrücken, dass es keinen Unterschied zwischen 2 und n gibt, wenn wir uns nur anschauen, ob die Zahl gerade ist, also ob die Zahl ein Vielfaches von 2 ist. Deswegen auch $\pmod 2$ für Vielfache von 2, bei Vielfachen von 3 würde man $\pmod 3$ schreiben.

Jetzt ist die Menge aller Zahlen für die gilt $k \equiv 2 \pmod 2$, die Menge aller geraden Zahlen

$$\{\, 2i \mid i \in \mathbb{Z} \,\} = 2\mathbb{Z}$$

(Es sind auch negative Zahlen enthalten)

Die Menge aller Zahlen für die gilt $k \equiv 1 \pmod 2$ ist die Menge aller ungeraden Zahlen

$$\{\, 2i + 1 \mid i \in \mathbb{Z} \,\} = 2\mathbb{Z} + \{\, 1 \,\}$$

Diese beiden Mengen sind die Restklassen, bzw. auch die Äquivalenzklassen unter $\equiv \pmod 2$.

Notiz 2.17. *Für* $\pmod 3$ *gilt übrigens, dass* $1 \not\equiv 2 \pmod 3$. *Das liegt daran, das* $2 + 1 \equiv 0 \pmod 3$, *aber* $1 + 1 \equiv 2 \not\equiv 0 \pmod 3$; 1 *und* 2 *sind also nicht gleich, wenn man sich nur Vielfachheit von* 3 *anschaut.*

Nun die formale Definition:

Definition 2.18. *Betrachten wir irgendeine Äquivalenzrelation* $\nsim$, *also eine Relation, die irgendeine Gleichheit angibt. Eine Äquivalenzrelation ist eine Relation, die*

- *transitiv ist*
$$\forall a, b, c : a \nsim b \land b \nsim c \implies a \nsim c$$
- *reflexiv ist*
$$\forall a : a \nsim a$$
- *symmetrisch ist*
$$\forall a, b : a \nsim b \iff b \nsim a$$

Definition 2.19. *Die Äquivalenzklasse von einem Element* a *bezüglich* $\nsim$ *ist*

$$[a]_{\nsim} = \{\, x \mid a \nsim x \,\}$$

also die Menge aller Elemente, die wir gegeneinander vertauschen können, wenn wir uns nur Gleichheit bezüglich $\nsim$ *betrachten.*

Beispiel 2.20.

- $\mathbb{C}$ *mit* $=$ *für* $\nsim$
$$[x]_{=} = \{\, x \,\}$$
es ist nur ein Element gleich zu sich selbst
- $\mathbb{N}$ *mit* $\equiv \pmod n$
$$[0]_{\equiv \pmod n} = n\mathbb{Z}$$
Wenn wir Vielfachheit von n *betrachten, dann sind alle Vielfachen von* n *gleich.*

Was sind nun genau die Äquivalenzklassen unter $\equiv \pmod n$? Wir könnten einfach sagen, dass dass nur [0] und [1] sind, damit fehlt uns allerdings eine sehr nützliche Eigenschaft: Verträglichkeit mit $+$ und $\cdot$

Also nochmal zum Beispiel $\equiv \pmod 3$

$$1 + 1 \equiv 2$$

$$2 + 1 \equiv 3 \equiv 0$$

Wenn aber $1 \equiv 2$:

$$0 \equiv 1 \equiv 2$$

Wenn wir Verträglichkeit mit $+$ und $\cdot$ wollen, dann müssen wir zwischen n verschiedenen Klassen unterscheiden:

$$\{\,[0], [1], \cdot, [n-1]\,\} = \{\,[k] \mid k \in \mathbb{Z}\,\} = \mathbb{Z}/n\mathbb{Z}$$

mit

$$[k] = \{\,k + in \mid i \in \mathbb{Z}\,\}$$

Wir haben außerdem folgende

Lemma 2.21. *Rechenregeln*
Für alle $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$ (Kommutativität):

$$\begin{array}{lcll} a + b & \equiv & b + a & (\text{mod } n) \\ a \cdot b & \equiv & b \cdot a & (\text{mod } n) \end{array}$$

Für alle $a, b, c \in \mathbb{Z}$ und $n \in \mathbb{N}$ (Assoziativität und Distributivität):

$$\begin{array}{lcll} (a + b) + c & \equiv & a + (b + c) & (\text{mod } n) \\ (a \cdot b) \cdot c & \equiv & a \cdot (b \cdot c) & (\text{mod } n) \\ a \cdot (b + c) & \equiv & ab + ac & (\text{mod } n) \end{array}$$

Wenden wir diesen neuen Stoff auf $n^2 + n + 1$ an:
Fall $n \equiv 0 \pmod 2$:
$n \equiv 0 \mid \cdot n$
Wir multiplizieren die Gleichung mit n.
$n^2 \equiv 0$
n^2 ist also gerade.
$n^2 \equiv 0 \mid +n$
$n^2 + n \equiv n$
Da $n \equiv 0$:
$n^2 + n \equiv 0$
$n^2 + n$ ist gerade.
$n^2 + n \equiv 0 \mid +1$
$n^2 + n + 1 \equiv 1$
Somit ist $n^2 + n + 1$ ungerade, falls n gerade ist.

Fall $n \equiv 1 \pmod 2$:
$n \equiv 1 \mid \cdot n$
$n^2 \equiv n \equiv 1$
$n^2 \equiv 1 \mid +n$
$n^2 + n \equiv 1 + n \equiv 1 + 1 \equiv 2 \equiv 0$

$n^2 + n \equiv 0 \mid +1$
$n^2 + n + 1 \equiv 1$
Somit ist $n^2 + n + 1$ ungerade, falls n gerade ist.

Somit ist $n^2 + n + 1$ immer ungerade!

2.6 Gruppen

Definition 2.22. *$(M, \circ)$ ist eine Gruppe mit M eine Menge und $\circ : M \times M \to M$, wenn folgendes gilt:*

- *Die Operation $\circ$ ist Assoziativ*

$$\forall a, b, c \in M : (a \circ b) \circ c = a \circ (b \circ c)$$

- *Es gibt ein neutrales Element wofür ich oft e_M schreiben werde*

$$\exists e_M \in M : \forall a \in M : e_M \circ a = a$$

- *Es gibt inverse Elemente a^{-1}*

$$\forall a \in M : \exists a^{-1} : a \circ a^{-1} = e_M$$

Gruppen $(M, \circ)$ nennt man zusätzlich noch abelsch, falls $\circ$ kommutiert, also $a \circ b = b \circ a$

Beispiel 2.23.

- $(\mathbb{Z}, +)$
- $(\mathbb{R}, \cdot)$ *und* $(\mathbb{Q}, \cdot)$
- $(\mathbb{Z}/n\mathbb{Z}, +)$

Diese Gruppen sind tatsächlich auch alle abelsch.

$(\mathbb{Z}/n\mathbb{Z} \setminus [0], \cdot)$ ist im allgemeinen keine Gruppe, betrachten wir z.B.$(\mathbb{Z}/4\mathbb{Z} \setminus [0], \cdot)$: Hier wäre das neutrale Element [1], da $x \cdot 1 = x$, allerdings gibt es kein 2^{-1} mit $2 \cdot 2^{-1} = 1$.

Beispiel 2.24. *Sei $(\mathbb{Z}/n\mathbb{Z})^* = \{ [k] \mid k, n \text{ coprim} \}$, dann ist $((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$ eine Gruppe:*

- *Die Multiplikation $\cdot$ ist assoziativ*
- *Das neutrale Element ist 1 und ist immer coprim zu n*
- *Inverse existieren tatsächlich auch immer*

Übrigens gilt für die Größe dieser Gruppe $|(\mathbb{Z}/n\mathbb{Z})^*| = \phi(n)$.

2.7 Ringe

Wieso schreiben wir nun $(\mathbb{Z}/n\mathbb{Z})^*$? Der Grund: auf $\mathbb{Z}/n\mathbb{Z}$ kann man immer eine Struktur bilden, die sich Ring nennt. Es gibt dann immer zwei Operationen (wie bei Körpern), die man oft $+$ und $\cdot$ schreibt.

Ein Ring sieht dann so aus: $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$

Nun ist $+$ das normale $+$, es ist assoziativ, kommutativ und invertierbar. Anders ist es mit $\cdot$, das muss nicht kommutativ und nicht invertierbar sein.

Wenn wir nun $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)^*$ schreiben (oder auch einfach $(\mathbb{Z}/n\mathbb{Z})^*$), dann meinen wir damit die größtmögliche Teilmenge von $\mathbb{Z}/n\mathbb{Z}$, die unter $\cdot$ eine Gruppe bildet, bzw. meinen wir damit diese Gruppe.

Dass diese immer existiert will ich kurz demonstrieren, nehmen wir $\mathcal{R}$ als beliebigen Ring: Betrachten wir $M = \{\, x \in \mathcal{R} \mid \exists y \in \mathcal{R} : xy = 1_{\mathcal{R}} \,\}$. $1_{\mathcal{R}}$ ist hier das neutrale Element von $\mathcal{R}$ bezüglich der Multiplikation.

Wir wissen, dass

- Die Multiplikation assoziativ ist
- Es existieren immer inverse (nach Definition)
- Es gibt ein neutrales Element, nämlich $1_{\mathcal{R}}$, was natürlich auch in M enthalten ist, da $1_{\mathcal{R}}$ immer $1_{\mathcal{R}} \cdot 1_{\mathcal{R}} = 1$ als inverses hat.

Somit ist M eine Gruppe,

2.8 Homomorphismen

Diese sind sehr ähnlich zu linearen Abbildungen auf Vektorräumen, betrachten beliebige Gruppen $(A, \circ)$ und $(B, \star)$. Eine Abbildung $T : A \to B$ ist ein Homomorphismus von A auf B, wenn für alle $x, y \in A$:

$$T(x \circ y) = T(x) \star T(y)$$

Wie bei linearen Abbildungen kann man den Kern $\ker T$ definieren:

$$\ker T = \{\, a \in A \mid T(a) = e_B \,\}$$

also alle Elemente, die auf das neutrale Element abgebildet werden.

Tatsächlich, wie bei lin. Abb., gilt T bijektiv $\iff$ $kerT = \{\, e_A \,\}$. Falls T bijektiv ist, nennen wir T auch einen Isomorphismus und schreiben $A \cong B$, da A und B auf gewisse Art und Weise einfach gleich sind. (z.B.haben sie dann immer einander entsprechende Elemente)

Betrachten wir eine interessante Eigenschaft von $\ker T$, denn für jedes $b \in B$ mit $\exists a \in A : T(a) = b$:

$$|T^{-1}(b)| = |\ker T|$$

Kurzer Beweis: Sei $k \in kerT$ beliebig, dann $T(a \circ k) = b \star e_B$. Da jedes $a \circ k$ unterschiedlich ist von jedem anderen muss $|T^{-1}(b)| \geq |\ker T|$, die Gleichheit gilt auch, allerdings will ich diese hier nicht beweisen.

2.9 Primitive Elemente

Definition 2.25. *Ein primitives Element einer Gruppe $(M, \circ)$ ist ein $g \in M$, sodass für jedes $x \in M$:*

$$\exists n \in N : x = g^n$$

g^n ist hier einfach die n-fache Ausführung von $\circ$. z.B.$g^2 = g \circ g$ und $g^1 = g$.

Man nennt g auch einen Generator von $(M, \circ)$.

Nicht alle Gruppen haben primitive Elemente, wenn sie eins haben, dann nennt man diese Gruppen zyklisch.

Satz 2.26. *Sei $(M, \circ)$ eine zyklische Gruppe mit $|M| = m < \infty$*

$$M \cong \mathbb{Z}/m\mathbb{Z}$$

Wenn wir also zyklische Gruppen studieren wollen, können wir genauso gut $\mathbb{Z}/m\mathbb{Z}$ studieren.

Beispiel 2.27. *Wir wollen wissen, wie viele primitive Elemente eine endliche zyklische Gruppe $(M, \circ)$ hat.*

Nun haben wir $M \cong \mathbb{Z}/m\mathbb{Z}$, was bedeutet, dass diese Gruppen bis auf eine Umbenennung der Elemente gleich sind.

Dadurch wissen wir, dass die Anzahl der primitiven Elemente in beiden Gruppen gleich sein muss. Was sind die primitiven Elemente von $\mathbb{Z}/m\mathbb{Z}$?

Die Zahlen, die coprim zu m sind.

Somit ist die Anzahl an primitiven Elementen in $\mathbb{Z}/m\mathbb{Z}$ und damit auch in M:

$$\phi(m)$$

Hier wieder die Euler-ϕ-Funktion.

Notiz 2.28. *Da $\mathbb{Z}/m\mathbb{Z}$ abelsch ist und $\mathbb{Z}/m\mathbb{Z} \cong M$ ist auch M abelsch.*

Jede zyklische Gruppe ist abelsch.

2.10 Ordnung

Definition 2.29. *Sei $(M, \circ)$ eine Gruppe. Für $x \in M$ nennen wir* $\mathrm{ord}(x)$ *die Ordnung von x und meinen damit die kleinste Zahl $n \in \mathbb{N}$ mit $x^n = e_M$.*

z.B.falls M zyklisch ist, gilt für primitive Elemente g:

$$\mathrm{ord}(g) = |M|$$

Es gilt beispielsweise auch immer $\mathrm{ord}(e_M) = 1$

Satz 2.30 (Satz von Lagrange)**.** *Für alle $x \in M$:*

$$\operatorname{ord}(x) \mid |M|$$

Es gibt auch eine stärkere Variante wenn M zyklisch ist, also primitive Elemente besitzt.

Satz 2.31. *Sei g ein primitives Element von M und $x \in M$, dann nennen wir $\log_g(x)$ die kleinste Zahl aus $\mathbb{N}$ mit $g^{\log_g(x)} = x$. Nun gilt*

$$\operatorname{ord}(x) \cdot \gcd(\log_g(x), |M|) = |M|$$

2.11 Direkte Summe

Hier wird es so richtig interessant!

Mit dem Isomorphismus zwischen zyklischen Gruppen und $\mathbb{Z}/m\mathbb{Z}$ lassen sich viele Fragestellungen auf sehr viel einfachere Strukturen reduzieren. Aber was ist, wenn wir nur eine abelsche Gruppe $(M, \circ)$ haben, die nicht zyklische ist? Hier kommt die direkte Summe $\oplus$ ins Spiel:

Definition 2.32. *Seien $(A, \circ)$ und $(B, \star)$ zwei abelsche Gruppen, dann ist $(A, \circ) \oplus (B, \star)$ (oder kurz $A \oplus B$) folgende Gruppe:*

- *Die Menge ist $A \times B$, das kartesische Produkt beider Mengen, die Menge aller möglichen Paare*
- *Die Gruppenoperation $\heartsuit : A \times B \to A \times B$ mit*

  $$(a_1, b_1) \heartsuit (a_2, b_2) \mapsto (a_1 \circ a_2, b_1 \star b_2)$$

  ist einfach nur die komponentenweise Anwendung der einzelnen Gruppenoperationen

Somit $A \oplus B = (A \times B, \heartsuit)$. Für $A \oplus A \oplus A$ schreiben wir A^3.

Nun was könnte die viel einfachere Struktur aus der Einleitung sein?

Satz 2.33. *Jede abelsche Gruppe $(M, \circ)$ lässt sich als direkte Summe von zyklischen Gruppen schreiben:*

$$M \cong \bigoplus_{p \in \mathbb{P}} \bigoplus_{n \in \mathbb{N}} (\mathbb{Z}/p^n\mathbb{Z})^{\mu(p,n)}$$

Hier ist $\mu(p, n)$, wie oft die Gruppe $\mathbb{Z}/p^n\mathbb{Z}$ in der Zerlegung auftaucht.

Die Gruppen $\mathbb{Z}/p^n\mathbb{Z}$ lassen sich übrigens nicht in weitere Gruppen zerlegen, somit ist auch die Zerlegung von M eindeutig (bis auf andere Reihenfolge bei der Summierung)

Lemma 2.34. *Seien $(A, \circ)$ und $(B, \star)$ zwei abelsche Gruppen und $a \in A$, $b \in B$, dann*

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

Beispiel 2.35. *Betrachten wir die abelsche aber nicht zyklische Gruppe $(\mathbb{Z}/15\mathbb{Z})^*$. Hierfür gilt*

$$(\mathbb{Z}/15\mathbb{Z})^* \cong (\mathbb{Z}/3\mathbb{Z})^* \oplus (\mathbb{Z}/5\mathbb{Z})^*$$

Was übrigens aus einem wichtigen Theorem namens Chinesischer Restsatz folgt.

Satz 2.36 (Chinesischer Restsatz)**.** *Sei $a, b \in \mathbb{N}$ mit a und b comprim. Nun ist*

$$\gamma : \mathbb{Z}/a\mathbb{Z} \oplus b \to \mathbb{Z}/a\mathbb{Z}b$$

mit

$$(\mathfrak{a}, \mathfrak{b}) \mapsto \mathfrak{ab}$$

ist immer ein Isomorphismus.

Wenn man nun γ einschränkt:

$$\beta : (\mathbb{Z}/a\mathbb{Z})^* \oplus (\mathbb{Z}/b\mathbb{Z})^* \to (\mathbb{Z}/ab\mathbb{Z})^*$$

mit $\beta(x) = \gamma(x)$ für alle $x \in (\mathbb{Z}/a\mathbb{Z})^* \oplus (\mathbb{Z}/b\mathbb{Z})^*$ dann erhält man wiederum einen Isomorphismus.

Nehmen wir für dieses Beispiel nun die Aufgabe, eine Menge $M \subset (\mathbb{Z}/15\mathbb{Z})^*$ zu finden, sodass man jedes $x \in (\mathbb{Z}/15\mathbb{Z})^*$ als Kombination von Elementen aus M unter Multiplikation (der Gruppenoperation) schreiben kann.

Da $(\mathbb{Z}/15\mathbb{Z})^*$ nicht zyklisch ist, muss $|M| > 1$.
Nun sind aber $(\mathbb{Z}/3\mathbb{Z})^*$ und $(\mathbb{Z}/1\mathbb{Z})^*5$ zyklisch mit jeweils 2 und 3 als generierenden Elementen.
Somit muss $\{(2, 1), (1, 3)\}$ eine generierende Menge von $(\mathbb{Z}/3\mathbb{Z})^* \oplus (\mathbb{Z}/5\mathbb{Z})^*$ sein, also dass man jedes Element von der Gruppe als Kombination schreiben kann.
Jetzt haben wir noch den Isomorphismus zu $(\mathbb{Z}/15\mathbb{Z})^*$, somit gibt es korrespondierende Elemente für $(2, 1)$ und $(1, 3)$.
Was sind diese Elemente?
Unter einem Isomorphismus wie β wären dass $2 \cdot 1 = 2$ und $1 \cdot 3 = 3$. Somit $M = \{2, 3\}$

2.12 Die Direkte Summe und Ringe

In diesem Paper werde ich viel implizit mit der Direkten Summe von Ringen und dann der Multiplikativen Gruppe davon arbeiten: $(\mathbb{A} \oplus \mathbb{B})^*$. Deswegen möchte ich noch kurz die Verträglichkeit dieser beiden Operationen $\oplus$ und $(\square)^*$ beweisen.

Lemma 2.37. *Nehmen wir zwei Ringe $\mathbb{A}$ und $\mathbb{B}$.*

$$\mathbb{A}^* \oplus \mathbb{B}^* \cong (\mathbb{A} \oplus \mathbb{B})^*$$

Beweis.

$$
\begin{aligned}
&(\mathbb{A} \oplus \mathbb{B})^* \\
&\qquad \cong \{\, (a,b) \mid a,b \in \mathbb{A},\mathbb{B} \,\}^* \\
&\qquad \cong \{\, (a,b) \mid a,b \in \mathbb{A},\mathbb{B} \wedge (\exists a^{-1}, b^{-1} : a \cdot a^{-1} = 1_{\mathbb{A}} \wedge b \cdot b^{-1} = 1_{\mathbb{B}}) \,\} \\
&\qquad \cong \{\, (a,b) \mid a \in \mathbb{A}^* \wedge b \in \mathbb{B}^* \,\} \\
&\qquad \cong \mathbb{A}^* \oplus \mathbb{B}^*
\end{aligned}
$$

□

3 Einleitung

Worum geht es hier überhaupt? Gegeben eine beliebige Zahl $m \in \mathbb{N}$ und die zugehörige Multiplikationsabbildung $M : \mathbb{N} \to \mathbb{N}, x \mapsto mx$, was ist die Anzahl an Orbits modulo eine andere Zahl.

Ein Orbit ist die Menge aller Zahlen, die von einer bestimmten Zahl und die Anwendung von M erreicht werden können. z.B. sei der Zyklus von 1 z_1, dann

$$1 \in z_1$$

$$\forall x_0 \in z_1 : M(x_0) \in z_1$$

Nun fehlt noch der *modulo* Teil, also sei noch gegeben $n \in \mathbb{N}$. Dazu modifizieren wir noch $M_n : \mathbb{N} \to \mathbb{N}, x \mapsto mx \bmod n$. Jetzt dürfte auch die Definition von Orbits mehr Sinn ergeben, da diese jetzt endlich endlich sein müssen und nicht einfach nur aus Vielfachen von m bestehen.

3.1 Ein paar Beispiele

Wählen wir $m = 3$

Für $n = 1$ bekommen wir $\pmod 1$ mit $\mathbb{Z}/1\mathbb{Z} = \{\, [0] \,\}$ als Menge, die wir uns anschauen wollen. Dieser Fall ist trivial, da es nur einen möglichen Wert gibt und somit nur einen Orbit mit nur einem Element.
Für $n = 2$ bekommen wir $\pmod 2$ mit $\mathbb{Z}/2\mathbb{Z} = \{\, 0, 1 \,\}$
$M(0) = 0 \mod 2 = 0$
$M(1) = 3 \mod 2 = 1$
Somit $0 \mapsto 0$ und $1 \mapsto 1$ als die zwei Orbits.

Notiz 3.1. *Hier möchte ich gerne etwas Notation einführen, um den Orbits einen sinnvollen Namen zu geben:*

Falls $x, y \in \mathbb{Z}/n\mathbb{Z}$ im gleichen Orbit unter M_n liegen, dann werde ich in diesem Paper $x \mathrel{\overset{\circ}{=}}_{m,n} y$ schreiben und $x \mathrel{\overset{\not\circ}{=}}_{m,n} y$, falls nicht.

Sei also $[x]_{\overset{\circ}{=}_{m,n}}$ der Orbit von x unter M_n, also alle Zahlen, die von x aus mit M_n erreichbar sind (x inklusive).

Somit noch die Definition von Orbits

$$x \in [x]_{\overset{\circ}{=}_{m,n}}$$

$$\forall x_0 \in [x]_{\overset{\circ}{=}_{m,n}} : M_n(x_0) \in [x]_{\overset{\circ}{=}_{m,n}}$$

Für $n = 4$ bekommen wir $\pmod 4$ mit $\mathbb{Z}/4\mathbb{Z} = \{\, 0, 1, 2, 3 \,\}$
$M(0) = 0 \mod 4 = 0$
$M(1) = 3 \mod 4 = 3$
$M(2) = 6 \mod 4 = 2$
$M(3) = 9 \mod 4 = 1$
Somit sind die Orbits $\Omega_{3,4} = \{\, [0]_{\overset{\circ}{=}_{3,4}}, [1]_{\overset{\circ}{=}_{3,4}}, [2]_{\overset{\circ}{=}_{3,4}} \,\}$

Notiz 3.2. *Zu $\Omega_{m,n}$: Wenn es eindeutig ist, wird in diesem Artikel auch einfach Ω geschrieben*

Für $n = 8$ bekommen wir $\pmod 8$ mit $\mathbb{Z}/8\mathbb{Z} = \{\, 0, 1, 2, 3, 4, 5, 6, 7 \,\}$
$M(0) = 0$
$M(1) = 3$
$M(2) = 6$
$M(3) = 1$
$M(4) = 4$
$M(5) = 7$
$M(6) = 2$
$M(7) = 5$
Ok.... so langsam wird es schwierig, hier noch den Überblick zu behalten, also mal die Zyklen ausgeschrieben:
0
$1 \mapsto 3$
$2 \mapsto 6$
4
$5 \mapsto 7$ (hier ist auch immer implizit der Pfeil zurück zum Anfang dabei)
Somit sind die Zyklen $\Omega = \{\, [0]_{\overset{\circ}{=}_{3,4}}, [1]_{\overset{\circ}{=}_{3,4}}, [2]_{\overset{\circ}{=}_{3,4}}, [4]_{\overset{\circ}{=}_{3,4}}, [5]_{\overset{\circ}{=}_{3,4}} \,\}$ mit $|\Omega| = 5$

Nun versuchen wir das ganze Mal mit Gruppentheorie auszudrücken. Wählen wir $n \in \mathbb{P}$, denn dann ist $(\mathbb{Z}/n\mathbb{Z})^*$ immer zyklisch (Tatsächlich ist auch $((\mathbb{Z}/n^{\square}\mathbb{Z})^*, \cdot)$ immer zyklisch).
Nun ist

$$|\Omega| = \frac{|(\mathbb{Z}/n\mathbb{Z})^*|}{\operatorname{ord}(m)} = \frac{\phi(n)}{\operatorname{ord}(m)} = \frac{n-1}{m}$$

Beweis.

$$|[m]_{\overset{\circ}{=}_{m,n}}| = \operatorname{ord}(m)$$

Für jedes $x \in (\mathbb{Z}/n\mathbb{Z})^*$ können wir nun $[x]_{\overset{\circ}{=}_{m,n}}$ betrachten.
Entweder gilt $x \in [m]_{\overset{\circ}{=}_{m,n}}$, dann gilt $[m]_{\overset{\circ}{=}_{m,n}} = [x]_{\overset{\circ}{=}_{m,n}}$.

Oder $[x]_{\triangleq_{m,n}} = x[m]_{\triangleq_{m,n}}$.
Betrachten wir ein Element m^t aus $[m]_{\triangleq_{m,n}}$ mit $t \in \mathbb{N}$.
Nun gilt $x(mm^t) = m(xm^t)$, und $[x]_{\triangleq_{m,n}} = x[m]_{\triangleq_{m,n}}$.

□

Wie wir hier sehen können hängt $|\Omega|$ von $\text{ord}(m)$ in einer Gruppe $((\mathbb{Z}/\square\mathbb{Z})^*)$ ab, diesen Zusammenhang betrachten wir aber besser später. Fürs erste

4 Die Ordnung unter Homomorphismen

Betrachten wir zwei Gruppen $\mathbb{Z}/pn\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z}$ mit $n \in \mathbb{N}$ und $p \in \mathbb{P}$ und dazu den surjektiven Homomorphismus $\gamma : \mathbb{Z}/pn\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ mit $x \to x \bmod n$.

Lemma 4.1. *Für $\mathbb{Z}/m\mathbb{Z}$ mit $m \in \mathbb{N}$ gilt:*

$$\text{ord}(x) = \frac{m}{\gcd(x, m)}$$

Beweis. Wir suchen $\text{ord}(x)$, also das kleinste $k \in \mathbb{N}$ mit $kx \equiv 0 \pmod m$

$$kx \equiv 0 \pmod m \iff m \mid kx \iff m = \gcd(m, kx)$$
$$\iff k \mid \frac{m}{\gcd(m, x)}$$

Da $k \in [1, m]$, ist das kleinste k: $\frac{m}{gcd(x,m)}$ □

Betrachten wir alle $t \in \mathbb{Z}/n\mathbb{Z}$ mit $0 \le t < n$ und $t + in \in \mathbb{Z}/pn\mathbb{Z}$ mit $0 \le i < p$.
Versuchen wir nun $\text{ord}_{\mathbb{Z}/pn\mathbb{Z}}(t+in)$ in Abhängigkeit von $\text{ord}_{\mathbb{Z}/n\mathbb{Z}}(t)$ zu bestimmen ($\text{ord}_{\mathbb{Z}/n\mathbb{Z}}$ steht hier für die Ordnung in $\text{ord}_{\mathbb{Z}/n\mathbb{Z}}$):

$$\text{ord}_{\mathbb{Z}/pn\mathbb{Z}}(t + in) = \frac{pn}{\gcd(t + in, pn)}$$

$$\gcd(t + in, pn) = \gcd\left(t + in, p^{v_p(n)+1} \cdot \frac{n}{p^{v_p(n)}}\right)$$

$p^{v_p(n)+1}$ ist hier $p \cdot$ die p-Primfaktoren von n und $\frac{n}{p^{v_p(n)}}$ sind alle anderen Primfaktoren.

$$\gcd\left(t + in, p^{v_p(n)+1} \cdot \frac{n}{p^{v_p(n)}}\right) = \gcd\left(t + in, p^{v_p(n)+1}\right) \cdot \gcd\left(t + in, \frac{n}{p^{v_p(n)}}\right)$$

die Faktoren coprim sind, kann man die Terme auseinanderziehen.

$$\gcd\left(t + in, \frac{n}{p^{v_p(n)}}\right) = \gcd\left(t, \frac{n}{p^{v_p(n)}}\right)$$

$$\gcd(t + in, p^{v_p(n)+1}) = p^{\min(v_p(t+in), v_p(n)+1)}$$

Für $\min(v_p(t + in), v_p(n) + 1)$ ergeben sich folgende Fälle:

	$i = 0$	$i \neq 0$
$t = 0$	$v_p(n) + 1$	$v_p(n)$
$v_p(t) < v_p(n)$	$v_p(t)$	$v_p(t)$
$v_p(t) = v_p(n)$	$v_p(t)$	$\begin{cases} v_p(n) + 1 & \text{für ein } i \\ v_p(n) & \text{sonst} \end{cases}$

Für interessierte Lesende ist das außergewöhnliche $i \equiv -t \cdot n^{-1} \pmod{p}$.

Beweis für $i = 0 \wedge t = 0$.

$$\begin{aligned} \min\{\, v_p(t + in), v_p(n) + 1 \,\} &= \min\{\, v_p(0), v_p(n) + 1 \,\} \\ &= \min\{\, \infty, v_p(n) + 1 \,\} \\ &= v_p(n) + 1 \end{aligned}$$

□

Beweis für $i \neq 0 \wedge t = 0$.

$$\begin{aligned} \min\{\, v_p(in), v_p(n) + 1 \,\} &= \min\{\, v_p(n), v_p(n) + 1 \,\} \\ &= v_p(n) \end{aligned}$$

da $v_p(i) = 0$, weil $0 < i < p$. □

Beweis für $i = 0 \wedge t \neq 0$.

$$\min\{\, v_p(t), v_p(n) + 1 \,\} = v_p(t)$$

da $v_p(t) < \infty$, weil $t \neq 0$ und da $v_p(t) < v_p(n) - 1$, weil $0 < t < n$. □

Beweis für $i \neq 0 \wedge v_p(t) < v_p(n)$.

$$\begin{aligned} \min\{\, v_p(t + \underbrace{in}_{v_p(in) = v_p(n)}), v_p(n) + 1 \,\} &= \min\{\, v_p(t), v_p(n) + 1 \,\} \\ &= v_p(t) \end{aligned}$$

□

Beweis für $i \neq 0 \wedge v_p(t) = v_p(n)$.

$$\min\{\, v_p(t + in), v_p(n) + 1 \,\}$$

ist entweder $v_p(n)$ oder $v_p(n) + 1$.
Es ist $v_p(n) + 1$ genau dann, wenn $p^{v_p(n)+1} \mid t + in$. Da $t \mid n$ können wir schreiben

$p^{v_p(n)+1} \mid t(t + i \cdot n \cdot t^{-1})$.
$p^{v_p(n)} \mid t$ womit $p \mid t + i \cdot n \cdot t^{-1}$ äquivalent ist.
Dann mit Moduloschreibweise: $t + i \cdot n \cdot t^{-1} \equiv 0 \pmod{p}$
Da t nur ein additives Inverses hat in $\mathbb{Z}/p\mathbb{Z}$ und $n \cdot t^{-1}$ coprim zu p ist, kann die Aussage nur für ein $0 < i < p$ gelten.

□

Jetzt können wir die Ordnung so schreiben:

$$\operatorname{ord}_{\mathbb{Z}/pn\mathbb{Z}}(t + in) = \frac{pn}{\gcd(t, \frac{n}{p^{v_p(n)}}) \cdot p^{\min\{\, v_p(t+in), v_p(n)\,\}}}$$

Dieser Ausdruck ist nicht der praktischste in der Anwendung deswegen möchte ich eine Konstante einfügen:

$$\operatorname{ord}_{\mathbb{Z}/pn\mathbb{Z}}(t + in) = \mathfrak{c} \cdot \operatorname{ord}_{\mathbb{Z}/n\mathbb{Z}}(t)$$

nun die Werte für $\mathfrak{c}$:

	$i = 0$	$i \neq 0$
$t = 0$	1	p
$v_p(t) < v_p(n)$	p	p
$v_p(t) = v_p(n)$	p	$\begin{cases} 1 & \text{für ein } i \\ p & \text{sonst} \end{cases}$

Die Faktoren können Sie gerne selbst nachrechnen, die ursprüngliche Tabelle sollte da eine große Hilfe sein.

Versuchen wir nun dieses Prinzip anzuwenden für

5 $\operatorname{ord}(m)$ in $(\mathbb{Z}/p^k\mathbb{Z})^*$

mit $p \in \mathbb{P} \setminus \{\, 2 \,\}$ und $m, k \in \mathbb{N}$ mit $p \nmid m$.

Hierfür betrachten wir erst mal zwei endliche zyklische Gruppen $(\widehat{M}, \circ)$, $(M, \circ)$ und einen surjektiven Homomorphismus $\gamma : \widehat{M} \to M$.

Sei g ein primitives Element von $\widehat{M}$.

Lemma 5.1. *γg ist ein primitives Element von M.*

Beweis. Wir wissen

$$\widehat{M} = \{\, g^k \mid k \in \mathbb{N} \wedge k \in [0, |\, \widehat{M}|) \,\}$$

Da γ surjektiv ist, gilt $\gamma\widehat{M} = M$ und somit

$$M = \{\, (\gamma g)^k \mid k \in \mathbb{N} \wedge k \in [0, \mid \widehat{M}|) \,\}$$

□

Corollary 5.1.1. *Somit gilt auch*

$$\ker T = \{\, g^k \mid M \mid \mid k \in \mathbb{N} \wedge k \in [0, \frac{\widehat{M}}{M}) \,\}$$

da $\operatorname{ord}(\gamma g) = |M|$ *und somit* $(\gamma g)^k = e_M$

Corollary 5.1.2.

$$|M| \mid |\widehat{M}|$$

Nun können wir die Gruppen $(\mathbb{Z}/p^1\mathbb{Z})^*, (\mathbb{Z}/p^2\mathbb{Z})^*, (\mathbb{Z}/p^3\mathbb{Z})^*, \dots$ und $\operatorname{ord}(m)$ für ein beliebiges $m \in \mathbb{N}$ mit $p \nmid m$ betrachten. Es ist hier wichtig, dass $p \in \mathbb{P} \setminus \{\, 2 \,\}$, da

Satz 5.2.

$$(\mathbb{Z}/n\mathbb{Z})^* \textit{ zyklisch} \iff n = 1 \vee n = 2 \vee n = 4 \vee n = p^k \vee n = 2p^k \textit{ für } p \in \mathbb{P}$$

Was von Gauss bewiesen wurde.

Betrachten wir nun $\operatorname{ord}_{(\mathbb{Z}/p^{k+1}\mathbb{Z})^*}(x)$ *in Abhängigkeit von* $\operatorname{ord}_{(\mathbb{Z}/p^k\mathbb{Z})^*}$:

Wir wissen, da $p \neq 2$, dass $(\mathbb{Z}/p^k\mathbb{Z})^*$ und $(\mathbb{Z}/p^{k+1}\mathbb{Z})^*$ zyklisch sind und somit.

$$(\mathbb{Z}/p^k\mathbb{Z})^* \cong \mathbb{Z}/\phi(p^k)\mathbb{Z}$$
$$(\mathbb{Z}/p^{k+1}\mathbb{Z})^* \cong \mathbb{Z}/\phi(p^{k+1})\mathbb{Z}$$

Dieser Isomorphismus ist nicht kanonisch, es gibt also mehr als eine Bijektion zwischen den Gruppen. Somit legen wir ein beliebiges primitives Element g von $(\mathbb{Z}/p^{k+1}\mathbb{Z})^*$ fest und definieren die Bijektionen $\gamma_k : \mathbb{Z}/\phi(p^k)\mathbb{Z} \to (\mathbb{Z}/p^k\mathbb{Z})^*$ mit $l \mapsto g^l$. Nun haben wir $\gamma_k^{-1}(m \bmod p^k) \in \mathbb{Z}/p^k\mathbb{Z}$.

Nun stellt sich die Frage, ob $\operatorname{ord}(m)$ für bestimmte k irgendwann in einfache Muster fällt. Betrachten wir hierfür $p^{v_p(\gamma_k^{-1}(m \bmod p^k))}$. Der Faktor, um den es sich verändert ist:

	$i = 0$	$i \neq 0$
$t = 0$	p	1
$v_p(t) < v_p(n)$	1	1
$v_p(t) = v_p(n)$	1	$\begin{cases} p & \text{für ein } i \\ 1 & \text{sonst} \end{cases}$

also $\frac{p}{\mathfrak{c}}$.

$p^{v_p(\phi(p^k))}$ verändert sich auch immer um einen Faktor von p.

Falls also $v_p(\gamma_k^{-1}(m \bmod p^k)) < v_p(\phi(p^k))$ bleibt $v_p(\gamma^{-1}(m \bmod p^k))$ immer gleich, da $v_p(\phi(p^k))$ streng monoton wächst. Wie die *Senke* bei DFAs.

Falls $m \equiv 1 \pmod{p}$, also $\gamma_1^{-1}(m \bmod p) = 0$ gilt für jedes k:

$$v_p(\gamma_k^{-1}(m \bmod p^k)) = v_p(\gamma_{k-1}^{-1}(m \bmod p^{k-1})) \cdot \begin{cases} p & \text{falls } m \equiv 1 \pmod{p^{k-1}} \\ 1 & \text{falls } m \not\equiv 1 \pmod{p^{k-1}} \end{cases}$$

Ab dem kleinsten k für das gilt $m \not\equiv 1 \pmod{p^k}$ ist die Sequenz in der *Senke*.

Falls $m \equiv -1 \pmod{p}$, also $\gamma_1^{-1}(m \bmod p) = \frac{p-1}{2}$ gilt für jedes k:

$$v_p(\gamma_k^{-1}(m \bmod p^k)) = v_p(\gamma_{k-1}^{-1}(m \bmod p^{k-1})) \cdot \begin{cases} p & \text{falls } m \equiv -1 \pmod{p^{k-1}} \\ 1 & \text{falls } m \not\equiv -1 \pmod{p^{k-1}} \end{cases}$$

Ab dem kleinsten k für das gilt $m \not\equiv -1 \pmod{p^k}$ ist die Sequenz wieder in der *Senke*.

Die letzten $p-3$ Fälle sind etwas komplexer zu beschreiben, statt Gleichheit mit 1 oder -1 ist für $\cdot p$ Gleichheit mit der p-adischen Zahl z notwendig, für die gilt $z^{\gamma_1^{-1}(m \bmod p)}$. In anderen Worten, es gilt für jedes k:

$$v_p(\gamma_k^{-1}(m \bmod p^k)) = v_p(\gamma_{k-1}^{-1}(m \bmod p^{k-1})) \cdot \begin{cases} p & \text{falls } m^e \equiv 1 \pmod{p^{k-1}} \\ 1 & \text{falls } m^e \not\equiv 1 \pmod{p^{k-1}} \end{cases}$$

mit $e = \gamma_1^{-1}(m \bmod p)$. Ab dem kleinsten k für das gilt $m^e \not\equiv 1 \pmod{p^k}$ ist die Sequenz wieder in der *Senke*.

Kleiner fun fact: Die vorherigen beiden Fälle mit $m \equiv 1$ und $m \equiv -1$ kann man auch auf diese Weise schreiben.

Wie wir hier sehen, gibt es in jedem Fall ein k_0, sodass

$$\forall k \geq k_0 : m^e \not\equiv 1 \pmod{p^k}$$

Nun ergibt sich:

$$\operatorname{ord}_{(\mathbb{Z}/p^k\mathbb{Z})^*}(m) = \operatorname{ord}_{(\mathbb{Z}/p\mathbb{Z})^*}(m) \cdot p^{\max\{\,0, k-k_0+1\,\}}$$

da $e = \gamma_1^{-1}(m \bmod p) = \operatorname{ord}_{(\mathbb{Z}/p\mathbb{Z})^*}(m)$

Was hat das nun mit Orbits zu tun?

6 Die Verbindung zwischen ord und $|\Omega|$

Betrachten wir erst einmal für $m \in \mathbb{N}$, $p \in \mathbb{P}$ und $k \in \mathbb{N}^+$ mit $p \nmid m$ die Abbildung $M_{p^k} : \mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ mit $x \mapsto mx$. Stellen wir folgendes fest:

$$v_p(x) = v_p(M_{p^k}(x))$$

da $p \nmid m$. Somit lässt sich die Wertemenge von M_{p^k}, also $\mathbb{Z}/p^k\mathbb{Z}$, in k-Submengen aufteilen, die geschlossen unter der Anwendung von M_{p^k} sind.

Notiz 6.1. *Für eine Funktion $f : A \to B$ und $X \subset A$ ist $f|_X : X \to B$ die Einschränkung von f auf die Definitionsmenge X.*

Die Orbits von M_{p^k} sind also genau die Orbits von

$$M_{p^k}|_{\{\,[n\cdot p^0]|n\in\mathbb{Z}\,\}}, M_{p^k}|_{\{\,[n\cdot p^1]|n\in\mathbb{Z}\,\}}, M_{p^k}|_{\{\,[n\cdot p^2]|n\in\mathbb{Z}\,\}}, \dots$$
$$\dots, M_{p^k}|_{\{\,[n\cdot p^{k-1}]|n\in\mathbb{Z}\,\}}, M_{p^k}|_{\{\,[n\cdot p^k]|n\in\mathbb{Z}\,\}}$$

zusammengenommen, also die Orbits von den Zahlen für die $v_p(\square) = 1$, für die $v_p(\square) = 2, \dots$, für die $v_p(\square) = k-1$ und für die $v_p(\square) = k$.
Nun ist für jedes $0 \le k_\heartsuit \le k$ die Länge des Orbits von $mp^{k_\heartsuit}$

$$|[mp^{k_\heartsuit}]_{\triangleq}| = \operatorname{ord}_{(\mathbb{Z}/p^{k-k_\heartsuit}\mathbb{Z})^*}(m)$$

Was steht hier also? Die Länge des Orbits von $mp^{k_\heartsuit}$ ist, wie oft man M_{p^k} anwenden muss, bis man wieder $mp^{k_\heartsuit}$ erhält. ord ist, wenn man bei 1 anfängt, wie oft man mit m multiplizieren muss, bis man wieder 1 erhält.

Warum kann man hier das eine durch das andere ersetzen? Ein anschauliches Beispiel:
Sei $p = 10$ eine Primzahl und sei $m = 3$. Betrachten wir die Orbits $\Omega_{3,10^2}$.
Betrachten wir vor allem einen, den von 10:

$$10 \mapsto 30 \mapsto 90 \mapsto 70$$

Dies ist genau der von $1 \pmod{10}$:

$$1 \mapsto 3 \mapsto 9 \mapsto 7$$

nur multipliziert mit 10.
Der Grund hierfür ist ziemlich offensichtlich. Es ist egal, wenn wir mit 3 multiplizieren, ob noch Nullen an der Zahl hängen oder nicht. 10 ist nun keine Primzahl, aber das gleiche Prinzip lässt sich auch auf andere Basen anwenden.

Nun wissen wir für alle $p^{k_\heartsuit}$ die Länge des Orbits. Dies sagt uns auch die Länge aller anderen Orbits von $\square \cdot p^{k_\heartsuit}$. Nehmen wir ein $0 \le k_\heartsuit \le k$ und ein $x \notin [k_\heartsuit]_{\triangleq} = [mk_\heartsuit]_{\triangleq}$ mit $v_p(x) = k_\heartsuit$:

$$[x]_{\triangleq} = \{\, ox \mid o \in [k_\heartsuit]_{\triangleq} \,\}$$

D.h. die Länge aller Orbits mit gleicher Wertigkeit ist gleich, nämlich $\operatorname{ord}_{(\mathbb{Z}/p^{k-k_\heartsuit}\mathbb{Z})^*}(m)$.
Was ist dann die Anzahl der Orbits mit Wertigkeit $k_\heartsuit$? Die Anzahl an möglichen Werten durch die Länge eines Orbits: $\phi(p^{k-k_\heartsuit}) / \operatorname{ord}_{(\mathbb{Z}/p^{k-k_\heartsuit}\mathbb{Z})^*}(m)$.

Somit

$$
\begin{aligned}
&|\Omega_{m,p^k}| \\
&= \sum_{k_\heartsuit=1}^{k} \phi(p^{k-k_\heartsuit})/\operatorname{ord}_{(\mathbb{Z}/p^{k-k_\heartsuit}\mathbb{Z})^*}(m) + 1 \\
&= \sum_{k_\heartsuit=0}^{k-1} \phi(p^{k_\heartsuit})/\operatorname{ord}_{(\mathbb{Z}/p^{k_\heartsuit}\mathbb{Z})^*}(m) + 1 \\
&= \sum_{k_\heartsuit=0}^{k-1} \frac{(p-1)p^{k_\heartsuit-1}}{\operatorname{ord}_{(\mathbb{Z}/p\mathbb{Z})^*}(m)\cdot p^{\max(0,k_\heartsuit-k_0+1)}} + 1 \\
&= \frac{p-1}{\operatorname{ord}_{(\mathbb{Z}/p\mathbb{Z})^*}(m)} \sum_{k_\heartsuit=0}^{k-1} \frac{p^{k_\heartsuit-1}}{p^{\max(0,k_\heartsuit-k_0+1)}} + 1 \\
&= \frac{p-1}{\operatorname{ord}_{(\mathbb{Z}/p\mathbb{Z})^*}(m)} \sum_{k_\heartsuit=0}^{k-1} p^{k_\heartsuit-1-\max(0,k_\heartsuit-k_0+1)} + 1 \\
&= \frac{p-1}{\operatorname{ord}_{(\mathbb{Z}/p\mathbb{Z})^*}(m)} \sum_{k_\heartsuit=0}^{k-1} \frac{1}{p}^{\max(0,k_\heartsuit-k_0+1)+1-k_\heartsuit} + 1 \\
&= \frac{p-1}{\operatorname{ord}_{(\mathbb{Z}/p\mathbb{Z})^*}(m)} \sum_{k_\heartsuit=0}^{k-1} \frac{1}{p}^{\max(-k_\heartsuit,-k_0+2)} + 1 \\
&= \frac{p-1}{\operatorname{ord}_{(\mathbb{Z}/p\mathbb{Z})^*}(m)} \sum_{k_\heartsuit=0}^{k-1} p^{\min(k_\heartsuit,k_0-2)} + 1 \\
&= \frac{p-1}{\operatorname{ord}_{(\mathbb{Z}/p\mathbb{Z})^*}(m)} \left(\sum_{k_\heartsuit=0}^{\min(k-1,k_0-2)} p^{k_\heartsuit} + \sum_{\substack{k_\heartsuit= \\ \min(k-1,k_0-2)+1}}^{k-1} p^{k_0-2} \right) + 1 \\
&= \frac{p-1}{\operatorname{ord}_{(\mathbb{Z}/p\mathbb{Z})^*}(m)} \left(\sum_{k_\heartsuit=0}^{\min(k-1,k_0-2)} p^{k_\heartsuit} + (k-1-\min(k-1,k_0-2))p^{k_0-2} \right) + 1 \\
&= \frac{p-1}{\operatorname{ord}_{(\mathbb{Z}/p\mathbb{Z})^*}(m)} \left(\sum_{k_\heartsuit=0}^{\min(k-1,k_0-2)} p^{k_\heartsuit} - (-k+1+\min(k-1,k_0-2))p^{k_0-2} \right) + 1 \\
&= \frac{p-1}{\operatorname{ord}_{(\mathbb{Z}/p\mathbb{Z})^*}(m)} \left(\sum_{k_\heartsuit=0}^{\min(k-1,k_0-2)} p^{k_\heartsuit} - (\min(0,k_0-k-1))p^{k_0-2} \right) + 1 \\
&= \frac{p-1}{\operatorname{ord}_{(\mathbb{Z}/p\mathbb{Z})^*}(m)} \left(\sum_{k_\heartsuit=0}^{\min(k-1,k_0-2)} p^{k_\heartsuit} + \max(0,k-k_0+1)p^{k_0-2} \right) + 1 \\
&= \frac{p-1}{\operatorname{ord}_{(\mathbb{Z}/p\mathbb{Z})^*}(m)} \left(\frac{p^{\min(k,k_0-1)}-1}{p-1} + \max(0,k-k_0+1)p^{k_0-2} \right) + 1 \\
&= \frac{1}{\operatorname{ord}_{(\mathbb{Z}/p\mathbb{Z})^*}(m)} \left(p^{\min(k,k_0-1)} - 1 + (p-1)\max(0,k-k_0+1)p^{k_0-2} \right) + 1
\end{aligned}
$$

7 ord(m) in $(\mathbb{Z}/2^n\mathbb{Z})^*$

Nun zu einer interessanten Frage, warum haben wir im letzten Abschnitt nicht gleich die Formel auch für 2^n gezeigt? Die einfache Antwort ist, dass $(\mathbb{Z}/2^n\mathbb{Z})^*$ nicht zyklisch ist, allerdings lässt sich ein fast gleicher Beweis auch hier durchführen, was ich in dem folgenden Abschnitt machen werde.

Zuallererst benötigen wir hierfür die Struktur von $(\mathbb{Z}/2^n\mathbb{Z})^*$:
$\{3, -1\}$ ist ein generierendes System für $(\mathbb{Z}/2^n\mathbb{Z})^*$, also für jedes $x \in (\mathbb{Z}/2^n\mathbb{Z})^*$:

$$\exists a, b \in \mathbb{N} \cup \{0\}, a < 2^{n-1}, b < 2 : x \equiv 3^a \cdot (-1)^b \pmod{2^n}$$

Schritt 1; 3 ist ein primitives Element von $(\mathbb{Z}/2\mathbb{Z})^*, (\mathbb{Z}/4\mathbb{Z})^*$:

$$(\mathbb{Z}/2\mathbb{Z})^* = \{[1]\} : 1 \mapsto 1$$

$$(\mathbb{Z}/4\mathbb{Z})^* = \{[1], [3]\} : 1 \mapsto 3 \mapsto 1$$

Nun betrachten wir induktiv ord(3) und versuchen zu zeigen, dass

$$\text{ord}_{(\mathbb{Z}/2^n\mathbb{Z})^*} = 2^{n-2}$$

Nehmen wir an für $\text{ord}_{(\mathbb{Z}/2^n\mathbb{Z})^*}(3) = 2^{n-2}$:
Es gibt zwei Fälle.

- $\text{ord}_{(\mathbb{Z}/2^{n+1}\mathbb{Z})^*} = 2^{n-2}$
- $\text{ord}_{(\mathbb{Z}/2^{n+1}\mathbb{Z})^*} = 2^{n-1}$

Betrachten wir nun $v_p(3^{2^{n-2}} - 1)$ und $v_p(3^{2^{n-2}} + 1)$.
$v_p(3^1) + 1 = 2$ und $v_p(3^{2n}) + 1 = 1$ für $n \in \mathbb{N}$.
Für $n = 2$ gilt $v_p(3^{2^0} - 1) = v_p(3^1 - 1) = v_p(2) = 1$
Nehmen wir an, dass $v_p(3^{2^{n-2}} - 1) = n - 1$ mit $n > 2$:

$$\begin{aligned} v_p(3^{2^{n-1}} - 1) &= v_p((3^{2^{n-2}})^2 - 1^2) \\ &= v_p((3^{2^{n-2}} - 1)(3^{2^{n-2}} + 1)) \\ &= v_p((3^{2^{n-2}} - 1)) + v_p((3^{2^{n-2}} + 1)) \\ &= n - 1 + 1 = n \end{aligned}$$

Somit muss $v_p(3^{2^{n-2}}) = n - 1$.

Damit muss $3^{2^{n-2}} = 3^{\text{ord}_{(\mathbb{Z}/2^{2^{n-1}}\mathbb{Z})^*}} = 2^{n-1}$ und $\text{ord}_{(\mathbb{Z}/2^n\mathbb{Z})^*} > \text{ord}_{(\mathbb{Z}/2^{n-1}\mathbb{Z})^*}$. Also $\text{ord}_{(\mathbb{Z}/2^n\mathbb{Z})^*} = 2^{n-1}$, da $\text{ord}_{(\mathbb{Z}/2^{n-1}\mathbb{Z})^*} \mid \text{ord}_{(\mathbb{Z}/2^n\mathbb{Z})^*}$. □

Schritt 2; $\nexists x \in N : 3^x \equiv -1 \pmod{2^n}$:
Für $(\mathbb{Z}/8\mathbb{Z})^*$: $1 \mapsto 3 \mapsto 1$.
Allerdings $2^n - 1 \equiv -1 \pmod{8}$ □

Man kann $\mathrm{ord}_{(\mathbb{Z}/2^{n-2}\mathbb{Z})^*}(3)$ Werte als 3-er Potenz darstellen, wenn man dann noch mit -1 multipliziert, kann man

$$2 \cdot \mathrm{ord}_{(\mathbb{Z}/2^n\mathbb{Z})^*}(3) = 2 \cdot \mathrm{ord}_{(\mathbb{Z}/2\cdot 2^{n-2}\mathbb{Z})^*} = 2^{n-1} = |(\mathbb{Z}/2^{n-1}\mathbb{Z})^*|$$

verschiedene Werte darstellen.
Somit ist $\{\, 3, -1 \,\}$ ein generierendes System von $(\mathbb{Z}/2^n\mathbb{Z})^*$. □
Nun muss

$$(\mathbb{Z}/2^n\mathbb{Z})^* \cong \mathbb{Z}/2^{n-2}\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

Wählen wir folgenden Isomorphismus:

$$\gamma : 2^{n-2} \oplus \mathbb{Z}/2\mathbb{Z} \to (\mathbb{Z}/2^n\mathbb{Z})^*$$

$$(a, b) \mapsto 3^a \cdot (-1)^b$$

oder äquivalent:

$$t \mapsto 3^{t_1} \cdot (-1)^{t_2}$$

mit $t \in \mathbb{N}^2$ und für $t = (a, b)$, $t_1 = a$ und $t_2 = b$.
Wir wissen, dass $G = (\{\, [3^l]_{\equiv \pmod{2^n}} \mid l \in \mathbb{N} \,\}, \cdot) \cong (\mathbb{Z}/2^{n-2}\mathbb{Z}, +)$ und somit

$$\mathrm{ord}_{(\mathbb{Z}/2^n\mathbb{Z})^*}(m) = \mathrm{lcm}(\mathrm{ord}_{\mathbb{Z}/2^{n-2}\mathbb{Z}}({\gamma^{-1}}_1(m)), \mathrm{ord}_{\mathbb{Z}/2\mathbb{Z}}({\gamma^{-1}}_2(m)))$$

$$= \mathrm{lcm}(\mathrm{ord}_G(m), \mathrm{ord}_{\mathbb{Z}/2\mathbb{Z}}({\gamma^{-1}}_2(m)))$$

in der letzten Zeilen müsste man eigentlich $\mathrm{ord}_{\mathbb{Z}/2\mathbb{Z}}({\gamma|_{\gamma(G)}}^{-1}{}_2(m))$ schreiben, was allerdings etwas unübersichtlich ist.

$$\mathrm{ord}_{\mathbb{Z}/2\mathbb{Z}}({\gamma^{-1}}_2(m)) = \begin{cases} 1 & \text{falls } {\gamma^{-1}}_2(m) = 0 \\ 2 & \text{falls } {\gamma^{-1}}_2(m) = 1 \end{cases}$$

G allerdings, ist zyklisch, das heißt wir können die Tabelle für v_2 anwenden.

	$i = 0$	$i \neq 0$
$t = 0$	$v_2(n) + 1$	$v_2(n)$
$v_2(t) < v_2(n)$	$v_2(t)$	$v_2(t)$
$v_2(t) = v_2(n)$	$v_2(t)$	$\begin{cases} v_2(n) + 1 & \text{für ein i} \\ v_2(n) & \text{sonst} \end{cases}$

Allerdings ist $v_2(t) = v_2(n)$ nur möglich, wenn $t = 0$, somit kann man die letzte Zeile weglassen:

	$i = 0$	$i \neq 0$
$t = 0$	$v_2(n) + 1$	$v_2(n)$
$v_2(t) < v_2(n)$	$v_2(t)$	$v_2(t)$

Wir haben, wie in dem letzten Abschnitt, also wieder ein k_0 ab dem für alle $n \geq k_0$ gilt: ${\gamma^{-1}}_1(m) \neq 0$ oder auch $m \not\equiv 1 \pmod{2^n}$.
Wenn $m = 3^{\square} \cdot (-1)^0$, dann ist

$$\mathrm{ord}_{(\mathbb{Z}/2^n\mathbb{Z})^*}(m) = 2^{\max(0,n-k_0+1)}$$

Wenn $m = 3^{\square} \cdot (-1)^1$, dann ist

$$\mathrm{ord}_{(\mathbb{Z}/2^n\mathbb{Z})^*}(m) = \mathrm{lcm}(\mathrm{ord}_{(\mathbb{Z}/2^n\mathbb{Z})^*}(-1), \mathrm{ord}_{(\mathbb{Z}/2^n\mathbb{Z})^*}(-m))$$

Für $n \leq 1$ gilt $\mathrm{ord}_{(\mathbb{Z}/2^n\mathbb{Z})^*}(-1) = 1$.
Für $n \geq 2$ gilt $\mathrm{ord}_{(\mathbb{Z}/2^n\mathbb{Z})^*}(-1) = 2$.
Somit wenn $m = 3^{\square} \cdot (-1)^1$ und $n \geq 2$, dann ist

$$\mathrm{ord}_{(\mathbb{Z}/2^n\mathbb{Z})^*}(m) = \mathrm{lcm}(2, \mathrm{ord}_{(\mathbb{Z}/2^n\mathbb{Z})^*}(-m))$$

Das k_0 zu $-m$ ist einfach die kleinste natürliche Zahl k_0, ab die für alle $n \geq k_0$ gilt:
$m \not\equiv -1 \pmod{2^n}$.
Somit können wir unsere Definition von k_0 umschreiben zu $m \not\equiv \pm 1 \pmod{2^n}$.

Hiermit ergibt sich dann die Formel:

$$\mathrm{ord}_{(\mathbb{Z}/2^n\mathbb{Z})^*}(m) = \begin{cases} 1 & \text{falls } n = 1 \\ 2^{\max(0,n-k_0+1)} & \text{falls } m \equiv 1 \pmod 4 \\ \mathrm{lcm}(2, 2^{\max(0,n-k_0+1)}) & \text{falls } m \equiv -1 \pmod 4 \end{cases}$$

oder auch

$$\mathrm{ord}_{(\mathbb{Z}/2^n\mathbb{Z})^*}(m) = \begin{cases} 1 & \text{falls } n \leq 1 \\ 2 & \text{falls } m \equiv -1 \pmod{2^n} \\ 2^{\max(0,n-k_0+1)} & \text{sonst} \end{cases}$$

Nun alles zusammenführen in

8 $\operatorname{ord}_{(\mathbb{Z}/n\mathbb{Z})^*}(m)$

Sei $n = p^e \cdot x$ mit $p \in \mathbb{P}$, $e = v_p(n)$ und $x = \frac{n}{p^e}$ Betrachten wir nun den Isomorphismus $\gamma : (\mathbb{Z}/p^e\mathbb{Z})^* \times (\mathbb{Z}/x\mathbb{Z})^* \to (\mathbb{Z}/p^e x\mathbb{Z})^*$ mit $(a, b) \mapsto ab$. Dies ist ein Isomorphismus nach dem Chinesischen Restsatz, da p^e und x coprim.

In anderen Worten

$$(\mathbb{Z}/p^e\mathbb{Z})^* \oplus (\mathbb{Z}/x\mathbb{Z})^* \cong (\mathbb{Z}/p^e x\mathbb{Z})^*$$

Wir wissen somit auch, dass für alle $m \in (\mathbb{Z}/p^e x\mathbb{Z})^*$:

$$\operatorname{ord}_{(\mathbb{Z}/p^e x\mathbb{Z})^*}(m) = \operatorname{lcm}\left(\operatorname{ord}_{(\mathbb{Z}/p^e\mathbb{Z})^*}(m), \operatorname{ord}_{(\mathbb{Z}/x\mathbb{Z})^*}(m) \right)$$

Wenn wir nun die Primfaktorzerlegung $n = \prod_{p\in\mathbb{P}} p^{v_p(n)}$ betrachten, dann gilt:

$$\operatorname{ord}_{(\mathbb{Z}/n\mathbb{Z})^*}(m) = \operatorname{lcm}\{ \operatorname{ord}_{(\mathbb{Z}/p^{v_p(n)}\mathbb{Z})^*}(m) \mid p \in \mathbb{P} \}$$

Das gilt, da $(\mathbb{Z}/1\mathbb{Z})^* = \{ [0] \}$ und somit $\operatorname{ord}_{(\mathbb{Z}/1\mathbb{Z})^*}(m) = 1$.

Warum lcm über alle Primzahlen? Wir wenden praktisch γ für jedes der einzelnen $p \mid n$ an.

Versuchen wir uns nun am Hauptthema-

9 $|\Omega|$

Wir haben also $m \in \mathbb{N}$ und $n \in \mathbb{N}$ mit m und n coprim. Nun gilt:

$$|\Omega_{m,n}| = \sum_{t|n} \frac{\phi(\frac{n}{t})}{\operatorname{ord}_{(\mathbb{Z}/\frac{n}{t}\mathbb{Z})^*}(m)}$$

Dies ist die gleiche Formel wie für $|\Omega_{m,p^k}|$ nur für allgemeine Zahlen. Der Beweis funktioniert auch hier ähnlich, da m und n coprim sind und somit jeder Orbit eine feste v_p Wertigkeit hat. Hier ist nun die Wertigkeit für alle $p \mid n$ gleich. $\square$

Versuchen wir die Formel etwas zu vereinfachen:

$$\sum_{t|n} \frac{\phi(\frac{n}{t})}{\operatorname{ord}_{(\mathbb{Z}/\frac{n}{t}\mathbb{Z})^*}(m)}$$

$$= \sum_{t|n} \frac{\phi(\frac{n}{t})}{\operatorname{lcm}\{\operatorname{ord}_{(\mathbb{Z}/p^{v_p(n/t)}\mathbb{Z})^*}(m) \mid p \in \mathbb{P}\}}$$

$$= \sum_{t|n} \frac{\phi(t)}{\operatorname{lcm}\{\operatorname{ord}_{(\mathbb{Z}/p^{v_p(t)}\mathbb{Z})^*}(m) \mid p \in \mathbb{P}\}}$$

Trennen wir nun die Summe nach Primfaktoren auf

$$= \sum_{e_0=0}^{v_2(n)} \sum_{e_1=0}^{v_{p_1}(n)} \sum_{e_2=0}^{v_{p_2}(n)} \cdots \sum_{e_\square=0}^{v_{p_\square}(n)} \frac{\phi(t)}{\operatorname{lcm}\{\operatorname{ord}_{(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*}(m) \mid i \in \mathbb{N}_0\}}$$

mit $t = \prod_{i\in\mathbb{N}} p_i^{e_i}$

$$= \sum_{e_0=0}^{v_2(n)} \sum_{e_1=0}^{v_{p_1}(n)} \sum_{e_2=0}^{v_{p_2}(n)} \cdots \sum_{e_\square=0}^{v_{p_\square}(n)} \frac{\phi(\prod_{i\in\mathbb{N}} p_i^{e_i})}{\operatorname{lcm}\{\operatorname{ord}_{(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*}(m) \mid i \in \mathbb{N}_0\}}$$

alle p_i sind coprim

$$= \sum_{e_0=0}^{v_2(n)} \sum_{e_1=0}^{v_{p_1}(n)} \sum_{e_2=0}^{v_{p_2}(n)} \cdots \sum_{e_\square=0}^{v_{p_\square}(n)} \frac{\prod_{i\in\mathbb{N}} \phi(p_i^{e_i})}{\operatorname{lcm}\{\operatorname{ord}_{(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*}(m) \mid i \in \mathbb{N}_0\}}$$

Weiter zu vereinfachen wird sehr schnell sehr kompliziert, weswegen ich es in diesem Paper nicht versuchen werde.

Da nun das Thema dieses Papers geklärt ist, möchte ich noch eine Anwendung der Ergebnisse die Gruppenstruktur von $(\mathbb{Z}/n\mathbb{Z})^*$ und ein ungenutztes Lemma präsentieren.

10 Anwendungen

Die Formel für die Anzahl an Orbits bringt mich nicht auf irgendwelche Anwendungsmöglichkeiten, anders ist es allerdings mit der allgemeinen Formel für die Ordnung eines Elements. Es lässt sich daraus ein Algorithmus extrahieren, der für bestimmte Zahlen sehr viel schneller ist als bisherige. Der Vorteil der Methode dieses Papers ist, gegeben eine Zahl $n = \prod_{p\in\mathbb{P}} p^{v_p(n)}$, dass der Algorithmus auch sehr schnell ist für größere v_p, anders als z.B. die Implementation von `sympy` also Python.

Auf den folgenden Seiten ist meine Implementation der Methode dieses Papers in Python:

```
from math import gcd, lcm


def calculate_k0(integer, prime):
    """Compute the k0 value for the
    calculation of the multiplicative order.

    :param integer: The number of which we are
        trying to find the order
    :param prime: The prime
    :returns: The value for k0, the smallest exponent
        such that integer**k0 is
        no longer of a specific form
    """

    if gcd(integer, prime) != 1:
        raise ValueError("integer and prime"
                         + " should be coprime")

    if prime == 2:
        # The normal procedure won't work here,
        # because n_order(integer, 2)==1
        # for every integer
        k0 = 2

        while True:
            mask = (1 << k0) - 1  # 2**k0 - 1
            # Bit operations used here,
            # could also beimplemented using %
            if (integer & mask != 1
                    and -integer & mask != 1):
                break
            k0 += 1
        return k0

    base_order = n_order(integer, prime)

    k0 = 2
    # We are trying to find the smallest exponent,
    # so we are doing a simple linear scan
    while pow(integer, base_order, prime ** k0) == 1:
        k0 += 1

    return k0


```

```
47 def fast_order_prime_power(integer, prime, exponent):
48     """
49     Calculate the order of integer modulo prime**exponent
50     :param integer: The element
51          of the multiplicative group
52     :param prime: The base
53     :param exponent: The exponent
54     :returns: The multiplicative order
55     """
56 
57     if gcd(integer, prime) != 1:
58         raise ValueError("integer and "
59                          + "prime should be coprime")
60     if exponent < 1:
61         raise ValueError("exponent should"
62                          + " be larger than 0")
63 
64     k0 = calculate_k0(integer, prime)
65 
66     if prime == 2:
67         # powers of two have a couple of specialties
68         if exponent == 1: return 1
69         if (integer + 1) & ((1 << exponent) - 1) == 0:
70                 return 2
71 
72         base_order = 1
73     else:
74         base_order = n_order(integer, prime)
75 
76     return base_order
77         * prime ** (max(0, exponent - k0 + 1))
78 
79 
80 def fast_order(integer, modulo):
81     """Calculate the multiplicative
82         order of integer mod modulo.
83 
84     :param integer: The element of the
85                          multiplicative group
86     :param modulo: The mod of the group
87     :returns: The order of integer
88     """
89 
90     if gcd(integer, modulo) != 1:
91         raise ValueError("integer and"
92                  + "modulo should be coprime")
```

```
93
94      order = 1
95
96      for prime, exponent in factorint(modulo).items():
97          order = lcm(
98              order,
99              fast_order_prime_power(
100             integer, prime, exponent)
101         )
102
103     return order
```

Die `fast_order` Methode ist, bis auf den dahinterliegenden Algorithmus, äquivalent zu `n_order` von `sympy`.

Vergleichen wir nun die Laufzeit:

Element	Primzahl	Exponent	Zeit Normal	Zeit Schnell	Zeit Normal log_2	Zeit Schnell log_2
3	2	1	0.00	0.00	-17.3	-15.4
3	2	10	0.00	0.00	-14.8	-15.6
3	2	100	0.00	0.00	-13.7	-15.7
3	2	1000	0.00	0.00	-7.9	-15.3
3	2	10000	2.21	0.00	1.1	-13.5
2	3	1	0.00	0.00	-15.9	-15.2
2	3	10	0.00	0.00	-15.1	-15.0
2	3	100	0.00	0.00	-12.2	-14.1
2	3	1000	0.03	0.00	-5.0	-13.3
2	3	10000	19.82	0.00	4.3	-10.3

Element ist m, die Zahl mit der wir multiplizieren. Primzahl p und Exponent e sind $p^e = m$, das die Gruppe angibt $(\mathbb{Z}/p^e\mathbb{Z})^*$. Zeit Normal ist die Zeit (in Sekunden), die `n_order` für den Aufruf benötigt. Zeit Schnell ist die Zeit, die meine Implementation braucht. Die log Zeiten sind $\log_2(t)$, also der zweite Logarithmus von der Zeit t.

Folgender Code wurde verwendet, um die Tabelle zu erstellen:

```
1  from math import gcd, log2
2  from timeit import timeit
3
4  from sympy import n_order
5
6  print("| Element | Primzahl | Exponent | Zeit Normal | "
7        + "Zeit Schnell | log Zeit Normal | log Zeit Schnell |")
8  print("|" + "-:|" * 7)
9
10 for PRIME in [2, 3]:
```

```
    for EXPONENT in [10 ** n for n in range(5)]:
        for MULT in [2, 3]:
            if gcd(MULT, PRIME) != 1:
                continue

            t_a = timeit(
                lambda: n_order(MULT, PRIME ** EXPONENT),
                number=1
            )
            t_b = timeit(
                lambda: fast_order(MULT, PRIME ** EXPONENT),
                number=1
            )

            print(
                f"| {MULT} | {PRIME} | {EXPONENT} | "
                + f"{t_a:0.2f} | {t_b:0.2f} | "
                + f"{log2(t_a):0.1f} | {log2(t_b):0.1f} |")
```

11 Struktur von $(\mathbb{Z}/n\mathbb{Z})^*$

Ganz am Anfang dieses Papers habe ich die Direkte Summe eingeführt und dabei ein wichtiges Theorem vorgestellt:

$$M \cong \bigoplus_{p\in\mathbb{P}} \bigoplus_{k\in\mathbb{N}} (\mathbb{Z}/p^k\mathbb{Z})^{\mu(p,k)}$$

Versuchen wir nun die Werte von $\mu(p,k)$ in Abhängigkeit von n zu bestimmen. Durch den Chinesischen Restsatz wissen wir, dass

$$(\mathbb{Z}/n\mathbb{Z})^* \cong \bigoplus_{p\in\mathbb{P}} (\mathbb{Z}/p^{v_p(n)}\mathbb{Z})^*$$

Nun ist alles, was noch übrig ist, die Gruppen $(\mathbb{Z}/p^{v_p(n)}\mathbb{Z})^*$ maximal zu zerlegen. Für $p \in \mathit{Primes} \setminus \{2\}$

$$(\mathbb{Z}/p^{v_p(n)}\mathbb{Z})^* \cong \begin{cases} \mathbb{Z}/1\mathbb{Z} \\ (\mathbb{Z}/(p-1)\mathbb{Z}) \oplus (\mathbb{Z}/(v_p(n)-1)\mathbb{Z}) \end{cases} \quad \text{falls} \quad \begin{matrix} v_p(n) = 0 \\ v_p(n) > 0 \end{matrix}$$

Nun noch zu $p = 2$. Wir wissen ja bereits aus $\mathrm{ord}(m)$ in $(\mathbb{Z}/2^n\mathbb{Z})^*$

$$(\mathbb{Z}/2^{v_2(n)}\mathbb{Z})^* \cong \begin{cases} \mathbb{Z}/1\mathbb{Z} \\ (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/(v_2(n)-1)\mathbb{Z}) \end{cases} \quad \text{falls} \quad \begin{matrix} v_2(n) = 0 \\ v_2(n) > 0 \end{matrix}$$

Nun ist $\mathbb{Z}/p^n\mathbb{Z}$ nicht mehr zerlegbar, $\mathbb{Z}/(p-1)\mathbb{Z}$ aber möglicherweise schon.
Versuchen wir nun eine Formel aufzustellen:

$$\mu(p,k) = \text{if}(\!|v_p(n) = k+1|\!) + \sum_{\substack{q\in\mathbb{P}\\ q|n}} \text{if}(\!|v_p(q-1) = k|\!)$$

$\text{if}(\!|\square|\!)$ ist hier eine Funktion, die einen Wahrheitswert zu 1 oder 0 umwandelt:

$$\text{if}(\!|A|\!) = 1 \iff A$$

12 Appendix

Das folgende Lemma habe ich im Zuge des Beweises erstellt, habe es dann schlussendlich nicht gebraucht. Nun habe ich es trotzdem dem Paper angehangen, da ich es interessant finde.

12.1 Ω in $A \times B$

Wir haben zwei endliche Mengen A und B und zwei bijektive Abbildungen $\alpha : A \to A$ und $\beta : B \to B$. Da α und β bijektiv sind, müssen sich Orbits unter ihnen ergeben, schreiben wir diese als Ω_α und respektive Ω_β. Betrachten wir $M_{p^k}|_{\{\,[n\cdot p^\cdot]\,|n\in\mathbb{Z}\,\}} A \times B \to A \times B$ mit $(a,b) \mapsto (\alpha(a), \beta(b))$ und dessen Orbits $\Omega_{\alpha\times\beta}$.

Lemma 12.1.

$$|\Omega_{\alpha\times\beta}| = \sum_{\substack{\aleph\in\Omega_\alpha\\ \beth\in\Omega_\beta}} \gcd(|\aleph|, |\beth|)$$

Beweis. Seien $\aleph \in \Omega_\alpha$ und $\beth \in \Omega_\beta$:
Versuchen wir zu verstehen, wie viele Orbits es unter $\alpha \times \beta|_{\aleph\times\beth}$ gibt. Tatsächlich können wir $(\aleph \times \beth, \alpha \times \beta|_{\aleph\times\beth})$ als Gruppe sehen und somit

$$(\aleph \times \beth, \alpha \times \beta|_{\aleph\times\beth}) \cong (\aleph, \alpha) \oplus (\beth, \beta)$$

Sei für $x \in M$: $[x]_\alpha$ der Orbit von x unter α.
z.B. für $a \in \aleph$ gilt $[a]_\alpha = \aleph$
Betrachten wir nun $a \in \aleph$ und $b \in \beth$:

$$|[(a,b)]_{\alpha\times\beta|_{\aleph\times\beth}}| = \text{lcm}(|[a]_\alpha|, |[b]_\beta)|$$

was aus der Direkten Summe folgt. Somit wissen wir aber auch, dass

$$|[(a,b)]_{\alpha\times\beta|_{\aleph\times\beth}}| = \text{lcm}(|\aleph|, |\beth|)$$

und alle Zyklen unter $\alpha \times \beta|_{\aleph \times \beth}$ die gleiche Länge haben, womit die Anzahl genau

$$|\Omega_{\alpha \times \beta|_{\aleph \times \beth}}| = \frac{|\aleph||\beth|}{\operatorname{lcm}(|\aleph|, |\beth|)} = \gcd(|\aleph|, |\beth|)$$

sein muss.

Wenn wir nun die Summe über alle $\aleph \in \Omega_\alpha$ und $\beth \in \Omega_\beta$ nehmen, dann erhalten wir die Formel aus dem Lemma.

□