Ordnung eines Elements einer Gruppe

Die Ordnung einer Gruppe ist definitionsgemäß die Anzahl ihrer Elemente.
Ist G eine Gruppe und $x \in G$, so definiert man die Ordnung des Elements x als Ordnung der von x erzeugten Untergruppe.
Aus dem Satz von Lagrange folgt, daß die Ordnung eines Gruppenelements ein Teiler der Ordnung der Gesamtgruppe sein muß. Ist die Ordnung eines Gruppenelements gleich der Ordnung der Gesamtgruppe, so ist dieses Element Erzeuger der Gruppe. Umgekehrt ist natürlich auch die Ordnung eines Erzeugers einer Gruppe gleich der Gruppenordnung.

In der Vorlesung wurde gezeigt, daß für jedes Element x in einer endlichen Gruppe G gilt:
ord x = min $\left\{ n \in \mathbb{N} \;\middle|\; x^n = e \right\}$.

Gilt umgekehrt $x^n = e$, so muß n ein Vielfaches von ord x sein.
Setzen wir nämlich ord $x = n_0$ und führen die Division mit Rest $n = q\, n_0 + r$ durch mit $0 \leq r < n_0$, so ergibt sich $e = x^n = x^{q n_0 + r} = \left(x^{n_0}\right)^q x^r = e^q x^r = x^r$, also $x^r = e$. Wegen der Minimalität von n_0 kann r nicht positiv sein, also ist r=0, und demnach $n = q\, n_0$.

Beispiel:
Die Gruppe $\mathbb{Z}_{43}^*$ besitzt 42 Elemente. Für ein Element $x \in \mathbb{Z}_{43}^*$ ist daher ord x ein Teiler von $42 = 2 \cdot 3 \cdot 7$. Daher muß ord x einen der Werte 1, 2, 3, 6, 7, 14, 21, 42 annehmen.

Es gilt jedenfalls $x^{42} = 1$, denn der Exponent 42 ist ja ein Vielfaches von ord x. Wenn x kein Erzeuger von $\mathbb{Z}_{43}^*$ ist, also eine Ordnung kleiner als 42 besitzt, so ist ord x ein echter Teiler von 42, und daher ein Teiler von 6, 14, oder 21; also muß dann gelten $x^{21} = 1$ oder $x^{14} = 1$ oder $x^6 = 1$. Sind demnach x^{21}, x^{14}, x^6 alle von 1 verschieden, so ist x Erzeuger von $\mathbb{Z}_{43}^*$.

Berechnen wir ord x für
x=7: $7^2 = 6$, $7^3 = 6 \cdot 7 = 42 = -1$, $7^6 = 7^3 \cdot 7^3 = (-1)(-1) = 1$. Damit ist ord 7 = 6 !!
x=2: $2^2 = 4$, $2^7 = 128 = 3 \cdot 43 - 1 = -1$, $2^{14} = 2^7 \cdot 2^7 = (-1) \cdot (-1) = 1$. Damit ist ord 2 = 14.

x=3: $3^2 = 9$, $3^4 = 81 = 2 \cdot 43 - 5 = -5$, $3^6 = 9 \cdot (-5) = -45 = -2$, $3^7 = (-2) \cdot 3 = -6$,
$3^{14} = (-6) \cdot (-6) = 36 = -7$, $3^{21} = (-7) \cdot (-6) = 42 = -1$.
Also sind 3^6, 3^{14} und 3^{21} alle drei von 1 verschieden und damit ord 3=42, und damit ist 3 Erzeuger von $\mathbb{Z}_{43}^*$.

Mit Hilfe eines Erzeugers können wir Elemente jeder möglichen Ordnung produzieren:

$3^0 = 1$ besitzt die Ordnung 1, $3^{21} = -1$ besitzt die Ordnung 2, $3^{14} = -7$ besitzt die Ordnung 3,
$3^7 = -6$ besitzt die Ordnung 6, $3^6 = -2$ besitzt die Ordnung 7, $3^3 = 27$ besitzt die Ordnung 14,
$3^2 = 9$ besitzt die Ordnung 21.

Die Elemente 3^n mit ggT(n,42)=1 sind sämtlich Erzeuger von $\mathbb{Z}_{43}^*$, und jeder Erzeuger von $\mathbb{Z}_{43}^*$ besitzt diese Form.
Sei dazu $x = 3^n$ mit ggT(n,42)=1. Wäre ord $x = k < 42$, hätte man $1 = x^k = (3^n)^k = 3^{nk}$, so müßte $n \cdot k$ ein Vielfaches von 42 sein. Mit Hilfe des Erweiterten Euklidischen Algorithmus können wir schreiben: $1 = n \cdot a + 42\, b$; daraus ergibt sich $k = n \cdot k \cdot a + 42 \cdot k \cdot b$; die rechte Seite dieser Gleichung ist dann offenbar durch 42 teilbar und die linke nicht. Widerspruch!
Ist umgekehrt x ein Erzeuger von $\mathbb{Z}_{43}^*$, so gibt es ein $n \in \mathbb{N}$ mit $3^n = x$ und $1 \leq n < 42$, denn 3 ist ja

ebenfalls ein Erzeuger. Wäre jetzt d:=ggT(n,42)>1, wobei $n = m \cdot d$, und $42 = d \cdot k$, so hätte man $x^m = (3^n)^k = 3^{n \cdot k} = 3^{m \cdot d \cdot k} = 3^{m \cdot 42} = (3^{42})^m = 1^m = 1$, was bedeutet, daß ord $x \leq m < 42$ so daß x kein Erzeuger sein könnte. Also muß ggT(42,n)=1 sein.

Wir haben also:
Ein Element der Form $x = 3^n$ mit ggT(n,42)=1 und $1 \leq n < 42$ ist Erzeuger von $\mathbb{Z}_{43}^*$, und jeder Erzeuger besitzt diese Form.

Dabei ist $n \in \{1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41\}$, und die Erzeuger von $\mathbb{Z}_{43}^*$ sind genau $3^1 = 3, 3^5 = 28, 3^{11} = 30, 3^{13} = 12, 3^{17} = 26, 3^{19} = 19, 3^{23} = 34, 3^{25} = 5, 3^{29} = 18, 3^{31} = 33, 3^{37} = 20, 3^{41} = 29$
Alle diese Elemente besitzen die Ordnung 42.