Potenzieren im Modul $2^3 = 8$ $Basis^{Exponent} = Potenz$

Wir betrachten jetzt immer den Modul $\mathbb{Z}_m^*$, der die zu m teilerfremden Zahlen enthält. Als Rechenarten interessieren nur Multiplizieren und Potenzieren modulo m.

$\mathbb{Z}_7^*$

Exponent \ Basis	1	2	3	4	5	6
1	1	2	3	4	5	6
2	1	4	2	2	4	1
3	1	1	6	1	6	6
4	1	2	4	4	2	1
5	1	4	5	2	3	6
6	1	1	1	1	1	1

Potenztafel in $(\mathbb{Z}_7^*, \cdot)$.

Ablesen: $4^3 \equiv_7 1$

Selber rechnen:

$4^3 = 4^2 \cdot 4 = 16 \cdot 4 \equiv_7$

$2 \cdot 4 = 8 \equiv_7 1$

Noch ein Rechenbeispiel: $2^5 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32 = (28+4) \equiv_7 4$

Wir betrachten, wann in einer Spalte die 1 zum ersten Mal auftaucht.
Bei 6 in Zeile 2, bei 2 und 4 in Zeile 3, bei 3 und 5 erst in Zeile 6.
Zeile 6 enthält sogar nur die 1. Hier zeigt sich ein zentraler Begriff:

Definition: Das kleinste k, das $a^k \equiv 1$ erfüllt heißt Ordnung des Elementes a.

Also hat 6 die Ordnung 2, dagegen haben 2 und 4 die Ordnung 3, aber 3 und 5 haben die Ordnung 6.

Darum gilt für jedes a mit Ordnung k: $a^{n\,k\,+r} \equiv a^r$ mit beliebigem n und r

Beispiel ausführlich $4^{17} = 4^{15+2} \equiv 4^{3 \cdot 5} \cdot 4^2 = (4^3)^5 \cdot 4^2 \equiv_7 1^5 \cdot 4^2 \equiv 4^2 \equiv_7 2$

Also kann man im Exponenten Vielfache der Ordnung weglassen.
Dann geht es schneller:

$ord(2) = 3 \Rightarrow 2^3 \equiv_7 1 \Rightarrow 2^{330} \equiv_7 1 \Rightarrow 2^{332} = 2^{330+2} \equiv_7 2^2 = 4$

$ord(5) = 6 \Rightarrow 5^{70} = 5^{66+4} \equiv_7 5^4 \equiv_7 2$

Kurz gesagt: In den Exponenten rechnet man modulo der Ordnung des Elementes.

Aufgabe: Stellen Sie die Potenztafeln von und $\mathbb{Z}_5^*$ und $\mathbb{Z}_{10}^*$ auf.

Berechnen Sie einige hohe Potenzen unter Ausnutzung der Elementordnung.
Prüfen Sie mit Excel oder anderen Mathematikwerkzeugen.