

Arbeitsblatt 3: Rechnen mit Kongruenzen

Aufgabe 3

Für verschiedene Werte von a und k sollen die Potenzen a^k modulo 7 berechnet werden. Vervollständige die Tabelle. Trage nur Zahlen zwischen 0 und 6 ein.

$k =$	1	2	3	4	5	6	7	
$2^k \equiv$	2	4	1	2	4	1	2	mod 7
$3^k \equiv$								mod 7
$4^k \equiv$								mod 7
$5^k \equiv$								mod 7
$6^k \equiv$								mod 7

Aufgabe 4

In der letzten Aufgabe hast Du Potenzen modulo 7 berechnet. Im Folgenden siehst Du einige Tabellen, in denen Potenzen a^k modulo verschiedener Zahlen m berechnet wurden.

- a) Betrachte in jeder Tabelle die unterste **Zeile**. Was fällt Dir auf? Stelle eine Formel auf, die Deine Beobachtung beschreibt.

Hinweis: Bezeichne die Zahl, bezüglich der die Modulo-Kongruenz berechnet wird, mit m . D.h. in der ersten Tabelle gilt $m = 5$ usw.

- b) Vergleiche die vorletzten **Spalten** der Tabellen miteinander. (Beachte auch die Tabelle für $m = 7$ aus der vorigen Aufgabe.) Was beobachtest Du? Schreibe als Text auf, was Du entdeckt hast. Kannst Du für spezielle Werte von m eine Formel für a^{m-1} angeben?

$k =$	1	2	3	4	5	
$0^k \equiv$	0	0	0	0	0	mod 5
$1^k \equiv$	1	1	1	1	1	mod 5
$2^k \equiv$	2	4	3	1	2	mod 5
$3^k \equiv$	3	4	2	1	3	mod 5
$4^k \equiv$	4	1	4	1	4	mod 5

$k =$	1	2	3	4	5	6	
$0^k \equiv$	0	0	0	0	0	0	mod 6
$1^k \equiv$	1	1	1	1	1	1	mod 6
$2^k \equiv$	2	4	2	4	2	4	mod 6
$3^k \equiv$	3	3	3	3	3	3	mod 6
$4^k \equiv$	4	4	4	4	4	4	mod 6
$5^k \equiv$	5	1	5	1	5	1	mod 6

$k =$	1	2	3	4	5	6	7	8	9	
$2^k \equiv$	2	4	8	7	5	1	2	4	8	mod 9
$3^k \equiv$	3	0	0	0	0	0	0	0	0	mod 9
$4^k \equiv$	4	7	1	4	7	1	4	7	1	mod 9
$5^k \equiv$	5	7	8	4	2	1	5	7	8	mod 9
$6^k \equiv$	6	0	0	0	0	0	0	0	0	mod 9
$7^k \equiv$	7	4	1	7	4	1	7	4	1	mod 9
$8^k \equiv$	8	1	8	1	8	1	8	1	8	mod 9

$k =$	1	2	3	4	5	6	7	8	9	10	
$2^k \equiv$	2	4	8	6	2	4	8	6	2	4	mod 10
$3^k \equiv$	3	9	7	1	3	9	7	1	3	9	mod 10
$4^k \equiv$	4	6	4	6	4	6	4	6	4	6	mod 10
$5^k \equiv$	5	5	5	5	5	5	5	5	5	5	mod 10
$6^k \equiv$	6	6	6	6	6	6	6	6	6	6	mod 10
$7^k \equiv$	7	9	3	1	7	9	3	1	7	9	mod 10
$8^k \equiv$	8	4	2	6	8	4	2	6	8	4	mod 10
$9^k \equiv$	9	1	9	1	9	1	9	1	9	1	mod 10

$k =$	1	2	3	4	5	6	7	8	9	10	11
$2^k \equiv$	2	4	8	5	10	9	7	3	6	1	2 mod 11
$3^k \equiv$	3	9	5	4	1	3	9	5	4	1	3 mod 11
$4^k \equiv$	4	5	9	3	1	4	5	9	3	1	4 mod 11
$5^k \equiv$	5	3	4	9	1	5	3	4	9	1	5 mod 11
$6^k \equiv$	6	3	7	9	10	5	8	4	2	1	6 mod 11
$7^k \equiv$	7	5	2	3	10	4	6	9	8	1	7 mod 11
$8^k \equiv$	8	9	6	4	10	3	2	5	7	1	8 mod 11
$9^k \equiv$	9	4	3	5	1	9	4	3	5	1	9 mod 11
$10^k \equiv$	10	1	10	1	10	1	10	1	10	1	10 mod 11

$k =$	1	2	3	4	5	6	7	8	9	10	11	12	13
$2^k \equiv$	2	4	8	3	6	12	11	9	5	10	7	1	2 mod 13
$3^k \equiv$	3	9	1	3	9	1	3	9	1	3	9	1	3 mod 13
$4^k \equiv$	4	3	12	9	10	1	4	3	12	9	10	1	4 mod 13
$5^k \equiv$	5	12	8	1	5	12	8	1	5	12	8	1	5 mod 13
$6^k \equiv$	6	10	8	9	2	12	7	3	5	4	11	1	6 mod 13
$7^k \equiv$	7	10	5	9	11	12	6	3	8	4	2	1	7 mod 13
$8^k \equiv$	8	12	5	1	8	12	5	1	8	12	5	1	8 mod 13
$9^k \equiv$	9	3	1	9	3	1	9	3	1	9	3	1	9 mod 13
$10^k \equiv$	10	9	12	3	4	1	10	9	12	3	4	1	9 mod 13
$11^k \equiv$	11	4	5	3	7	12	2	9	8	10	6	1	11 mod 13
$12^k \equiv$	12	1	12	1	12	1	12	1	12	1	12	1	12 mod 13