Potenzen und kleiner Satz von Fermat

Aufgabe 1

Berechne die folgenden Potenzen möglichst geschickt ohne Taschenrechner:

a) $[4]^{-11}$ in $\mathbb{Z}_{13}$:

b) $[6]^{31}$ in $\mathbb{Z}_{29}$:

c) $[6]^{32}$ in $\mathbb{Z}_{29}$:

Zusatzaufgabe 1

Für diese Aufgabe benützen wir eine Potenztabelle für $\mathbb{Z}_{11}$.

$k =$	1	2	3	4	5	6	7	8	9	10
$[2]^k =$	$[2]$	$[4]$	$[8]$	$[5]$	$[10]$	$[9]$	$[7]$	$[3]$	$[6]$	$[1]$
$[4]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

a) Trage in die Tabelle die Potenzen von $[4]$ in $\mathbb{Z}_{11}$ ein. Wie viele verschiedene Elemente von $\mathbb{Z}_{11}$ können durch $[4]^k$ dargestellt werden? Warum ist $[4]$ keine Primitivwurzel?

b) Wie hängen die Zeile für $[4]^k$ und die Zeile für $[2]^k$ zusammen?

c) Sei p eine Primzahl mit $p \geq 3$ und $[n^2]$ eine Quadratzahl in $\mathbb{Z}_p$ mit $[n] \neq 0$. Folgere aus dem kleinen Satz von Fermat dass $[n^2]^{(p-1)/2} = [1]$ gilt.

d) Sei p eine Primzahl mit $p \geq 3$. Wie viele verschiedene Elemente von $\mathbb{Z}_p$ können höchstens durch $[n^2]^k$ mit $k \in \mathbb{N}$ dargestellt werden? Warum ist $[n^2]$ keine Primitivwurzel?