

Schriftliche Aufgaben

Name:

Aufgabe 6

Berechne jeweils die Potenz in dem angegebenen Restklassenring \mathbb{Z}_m . Beachte, dass der kleine Satz von Fermat dann und nur dann angewandt werden kann, wenn m eine Primzahl ist.

a) In \mathbb{Z}_{29} : $[4]^{28} =$,

b) in \mathbb{Z}_{31} : $[17]^{94} =$,

c) in \mathbb{Z}_{12} : $[4]^{11} =$,

d) in \mathbb{Z}_{12} : $[3]^{12} =$.

Aufgabe 7

a) Berechne die angegebenen Potenzen in \mathbb{Z}_{13} und trage sie in die Tabelle ein.

Hinweis: Es dürfen nur Zahlen von 0 bis 12 eingetragen werden. Sobald die Restklasse $[1]$ erreicht ist, brauchst Du nichts mehr einzutragen.

$k =$	1	2	3	4	5	6
$[2]^k =$	[]	[]	[]	[]	[]	[]
$[3]^k =$	[]	[]	[]	[]	[]	[]
$[4]^k =$	[]	[]	[]	[]	[]	[]
$[5]^k =$	[]	[]	[]	[]	[]	[]

b) Welche der Restklassen $[2], [3], [4], [5]$ sind Primitivwurzeln?

In \mathbb{Z}_{13} sind Primitivwurzeln: .

Weiter auf Seite 2

Aufgabe 8

a) Berechne in \mathbb{Z}_{23} die angegebenen Brüche:

$$\frac{[2]}{[3]^{20}} = \boxed{}, \quad \frac{[5]}{[9]^{11}} = \boxed{}.$$

b) Gib jeweils 4 verschiedene Werte für k an, so dass die angegebene Gleichung in \mathbb{Z}_{31} gilt. Genau einer der k -Werte soll negativ sein.

$$[7]^k = [7]^3 \text{ für } k = \boxed{},$$

$$[16]^k = [16]^2 \text{ für } k = \boxed{},$$

Aufgabe 9

Andy und Berenice vereinbaren für den Schlüsseltausch $p = 11$ und $g = 6$. Andy schickt an Berenice die Zahl $A = 8$, Berenice meldet $B = 2$. Kurze Zeit später übermittelt Andy die Nachricht

k	m	l	s	k	h	l	o	i	n	e	p	z	b

a) Bestimme a , b und den Schlüssel K .

$$a = \boxed{}, \quad b = \boxed{}, \quad K = \boxed{},$$

b) Entschlüsse die Nachricht mit dem Zahlwort zu K als Schlüsselwort für Vigenère-Entschlüsselung.

Hinweis: Verwende die Tabelle der Potenzen $[6]^k$ aus Aufgabe 3b (Arbeitsblatt 6.3).