Arbeitsblatt 8

Kapitel 11: Kryptologie

Aufgabe 1

Gegeben ist die Äquivalenzklasse $[3]_7 = \{ \ldots, -11, -4, 3, 10, 17, \ldots \} = \{ 3 + k \cdot 7 : k \in Z \}$
Die Äquivalenzklassen $[-4]_7$ und $[10]_7$ sind mit $[3]_7$ identisch.

Schreiben Sie für jedes Element der Teilmenge {-18, -11, -4, 3, 10, 17, 24 } von $[3]_7$ die Quotienten q auf, welche bei Division durch 7 die Reste 3, -4 und 10 haben.

Aufgabe 2

Gegeben ist der Modul n=8 und der Rest r=5 mit $r \in [b]_n$. Schreiben Sie 5 negative und 5 positive Restklassen die mit $[b]_n$ identisch sind.

Schreiben Sie für die Restklassen auch die Quotienten q auf, welche die Reste bilden.

Aufgabe 3

Finden Sie durch Ausprobieren eine Primfaktorzerlegung für die Zahl a = 42 694 003 mit den Primzahlen 11, 23, 29.

Warum ist es so schwierig, für eine große beliebige Zahl eine Primfaktorzerlegung zu finden?