Arbeitsblatt 11

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?

Lösung 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.

Benutze das Divisonstheorem von Folie Kap 11.1/17: a / n = q Rest r

a : 7 = q Rest 3	**a :7 = q Rest -4**	**a : 7 = q Rest 10**
-18 : 7 = -3	-18 : 7 = -2	-18 : 7 = -4
-11 : 7 = -2	-11 : 7 = -1	-11 : 7 = -3
-4 : 7 = -1	-4 : 7 = 0	-4 : 7 = -2
3 : 7 = 0	3 : 7 = 1	3 : 7 = -1
10 : 7 = 1	10 : 7 = 2	10 : 7 = 0
17 : 7 = 2	17 : 7 = 3	17 : 7 = 1
24 : 7 = 3	24 : 7 = 4	24 : 7 = 2
31 : 7 = 4	31 : 7 = 5	31 : 7 = 3

Lösung 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.

$[5]_8 = \{ \ldots, -27, -19, -11, -3, 5, 13, 21, 29, 37, \ldots \}$

$[-27]_8 = [-19]_8 = [-11]_8 = [-3]_8 = [5]_8 = [21]_8 = \ldots$

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

…
1 * 8 + 5 = 13 q = 5
0 * 8 + 5 = 5 q = 0
-1 * 8 + 5 = -3 q = -8
-2 * 8 + 5 = -11 q = -16
-3 * 8 + 5 = -19 q = -24
-4 * 8 + 5 = -27 q = -32
…

…
0 * 8 - 3 = 13 q = 0
1 * 8 - 3 = 5 q = 8
2 * 8 - 3 = 13 q = 16
3 * 8 - 3 = 21 q = 24
4 * 8 - 3 = 29 q = 32

5 * 8 - 3 = 37 q = 40
…

Lösung Aufgabe 3

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

$42\,694\,003 = 11^2 * 23^3 * 29^1$