Aufgabe 1:

b)

```
? 4 + 7
%1 = 11
?
```

```
? gcd(98, 280)
%2 = 14
?
```

```
break[2]> 9746 % 17
5
break[2]>
```

Aufgabe 2:

$N = 143$

$e = 23$

$d = 47$

Verschlüsseln:

$$c \equiv m^e \pmod{N}$$

$$c \equiv g^{23} \pmod{143}$$

$$\underline{\underline{c \equiv 3}}$$

Entschlüsseln:

$$m \equiv c^d \pmod{N}$$

$$m \equiv 3^{47} \pmod{143}$$

$$m \equiv g$$

Aufgabe 3:

a) $\cup$ von 2 in $\mathbb{Z}_{17}^*$

$\rightarrow \{1, 2, 4, 8, 9, 13, 15, 16\}$

b) $2 \cdot x \equiv 1 \pmod{17} \Rightarrow 2^{-1} = 9$

```
break[2]> a = 2
2
break[2]> n = 17
17
break[2]> inverse = lift(Mod(a^(-1),n))
9
```

$9^5 \bmod 17 = \underline{8}$

c)(i) $|\mathbb{Z}_{1237}^*| = 1236 = 2 \cdot 2 \cdot 3 \cdot 103$

möglich Ordnungen:

2
3
103
1236

$2^{1236/2} = 2^{618} \pmod{1237} = 1236$

$2^{1236/3} = 2^{412} \pmod{1237} = 300$

$2^{1236/103} = 2^{12} \pmod{1237} = 385$

(1 9) ( )

Ordnung von	
2	1236
$2^2 = 4$	$\frac{1236}{2}$
2^x	$\frac{1236}{x}$

2 ist eine Primitivwurzel

(ii) $2^1 \rightarrow$ Ordnung 1236

$2^x \rightarrow$ Ordnung $\frac{1236}{x} = 103 \rightarrow \frac{1236}{103} = 12 = x$

$\underline{2^{12}}$ muss also die Ordnung 103 haben

4) a) $5 \cdot x \equiv 1 \pmod{17} = 7$

$5^{-7} \equiv 12$

$1 \cdot 3^{-1} = 3 \cdot x \equiv 1 \pmod{17} = 6$

$1 \cdot 3^{-1} \cdot 5^{-7} \equiv 6 \cdot 12 = \underline{72}$

b) $\frac{1}{2}\left(4x + \frac{1}{3}\right) = \frac{1}{4}(12x + 1)$

$2x + \frac{1}{6} = 3x + \frac{1}{4}$

$2x + \frac{2}{12} = 3x + \frac{3}{12}$

$x = -\frac{1}{12}$

$x = -1 \cdot 12^{-1} \mod 19$

$\underline{x = -8} \mod 19 = \underline{x = 11}$

5 a) $437 = 19 \cdot 23$

$\varphi(437) = 18 \cdot 22 = 396$

$1 < e < 396$

```
break[5]> not_divisors(n) = {
    list = [1];
    for(i=2, n-1,
        if(gcd(i, n) == 1,
            list = concat(list, i)
        )
    );
    return(list);
}
break[5]> not_divisors(396)
[1, 5, 7, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53, 59, 61, 65, 67, 71, 73, 79
, 83, 85, 89, 91, 95, 97, 101, 103, 107, 109, 113, 115, 119, 125, 127, 131, 133, 137, 139, 1
45, 149, 151, 155, 157, 161, 163, 167, 169, 173, 175, 179, 181, 185, 191, 193, 197, 199, 203
, 205, 211, 215, 217, 221, 223, 227, 229, 233, 235, 239, 241, 245, 247, 251, 257, 259, 263,
265, 269, 271, 277, 281, 283, 287, 289, 293, 295, 299, 301, 305, 307, 311, 313, 317, 323, 32
5, 329, 331, 335, 337, 343, 347, 349, 353, 355, 359, 361, 365, 367, 371, 373, 377, 379, 383,
 389, 391, 395]
break[5]> list = not_divisors(396)
[1, 5, 7, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53, 59, 61, 65, 67, 71, 73, 79
, 83, 85, 89, 91, 95, 97, 101, 103, 107, 109, 113, 115, 119, 125, 127, 131, 133, 137, 139, 1
45, 149, 151, 155, 157, 161, 163, 167, 169, 173, 175, 179, 181, 185, 191, 193, 197, 199, 203
, 205, 211, 215, 217, 221, 223, 227, 229, 233, 235, 239, 241, 245, 247, 251, 257, 259, 263,
265, 269, 271, 277, 281, 283, 287, 289, 293, 295, 299, 301, 305, 307, 311, 313, 317, 323, 32
5, 329, 331, 335, 337, 343, 347, 349, 353, 355, 359, 361, 365, 367, 371, 373, 377, 379, 383,
 389, 391, 395]
break[5]> print(#list)
120
```

Es gibt 120 Möglichkeiten

b) $\varphi(899) = (29-1) \cdot (31-1) = 28 \cdot 30 = \underline{840}$

$m \equiv c^d$ $\quad e \cdot d + k \cdot \varphi(N) = 1$

$m \equiv 400^d \mod 899$ $\quad e \cdot d + k \cdot 840 = 1$

$e = \text{Mod}(11, 840)$ $\quad 11 \cdot d + k \cdot 840 = 1$

e^{-1}

$\hat{=} 611$

✨ Erweiterter Euklidischer Algorithmus ✨

$d = 611$

$m \equiv c^d = 400^{611} \mod 899 = \underline{297}$

Überprüfung

$c \equiv m^e = 297^{11} \mod 899 = \underline{400}$