Aufgabe 9.1

(i) $3(x+3) \equiv 7 \bmod 13$

$\Leftrightarrow \quad 1(x+3) \equiv 11 \bmod 13$

$\Leftrightarrow \quad x \equiv 8 \bmod 13$

(ii) $17(2-x)x \equiv 4x^2 - x + 7 \bmod 21$ lässt sich zerlegen in:

$17(2-x)x \equiv 4x^2 - x + 7 \bmod 3$

$\Leftrightarrow \quad 34x - 17x^2 \equiv 4x^2 - x + 7 \bmod 3$

$\Leftrightarrow \quad x + x^2 \equiv x^2 + 2x + 1 \bmod 3$

$\Leftrightarrow \quad x \equiv 2x + 1 \bmod 3$

$\Leftrightarrow \quad x \equiv 2 \bmod 3$

$17(2-x)x \equiv 4x^2 - x + 7 \bmod 7$

$\Leftrightarrow \quad 34x - 17x^2 \equiv 4x^2 - x + 7 \bmod 7$

$\Leftrightarrow \quad 6x + 4x^2 \equiv 4x^2 + 6x \bmod 7$

$\Leftrightarrow \quad 0 \equiv 0 \bmod 7$

Also gibt es 7 Lösungen:
$\forall y \in \mathbb{N} \mid 0 \le y \le 6 : x \equiv y \bmod 7$

Die gemeinsamen Lösungen lasen sich jetzt mit dem Chinesischen Restsatz bestimmen:

$b_1 = 7$

$b_2 = 3$

$7x_1 \equiv 2 \bmod 3$

$\Leftrightarrow \quad x_1 \equiv 2 \bmod 3$

$3x_2 \equiv 0 \bmod 7 \vee 3x_2 \equiv 1 \bmod 7 \vee 3x_2 \equiv 2 \bmod 7 \vee 3x_2 \equiv 3 \bmod 7$
$\vee 3x_2 \equiv 4 \bmod 7 \vee 3x_2 \equiv 5 \bmod 7 \vee 3x_2 \equiv 6 \bmod 7$

$\Leftrightarrow \quad x_2 \equiv 0 \bmod 7 \vee x_2 \equiv 5 \bmod 7 \vee x_2 \equiv 3 \bmod 7 \vee x_2 \equiv 1 \bmod 7$
$\vee x_2 \equiv 6 \bmod 7 \vee x_2 \equiv 4 \bmod 7 \vee x_2 \equiv 2 \bmod 7$

$x \equiv 2 \cdot 7 + 0 \cdot 3 \equiv 14 \bmod 21 \quad \vee$

$x \equiv 2 \cdot 7 + 1 \cdot 3 \equiv 17 \bmod 21 \quad \vee$

$x \equiv 2 \cdot 7 + 2 \cdot 3 \equiv 20 \bmod 21 \quad \vee$

$x \equiv 2 \cdot 7 + 3 \cdot 3 \equiv 2 \bmod 21 \quad \vee$

$x \equiv 2 \cdot 7 + 4 \cdot 3 \equiv 5 \bmod 21 \quad \vee$

$x \equiv 2 \cdot 7 + 5 \cdot 3 \equiv 8 \bmod 21 \quad \vee$

$x \equiv 2 \cdot 7 + 6 \cdot 3 \equiv 11 \bmod 21 \quad \vee$

$L = \{2, 5, 8, 11, 14, 17, 20\}$

(iii) $x + \frac{1}{x} \equiv 1 - 5x \bmod 6$

$\Leftrightarrow \quad x^2 + 1 \equiv x - 5x^2 \bmod 6$

$\Leftrightarrow \quad 1 \equiv x - 6x^2 \bmod 6$

$\Leftrightarrow \quad x \equiv 1 \bmod 6$

(iv) $3x \equiv 9 \bmod 105$ lässt sich zerlegen in:

$$3x \equiv 9 \bmod 3 \quad\quad 3x \equiv 9 \bmod 5 \quad\quad 3x \equiv 9 \bmod 7$$

$$\Leftrightarrow \quad 0 \equiv 0 \bmod 3 \quad\quad \Leftrightarrow \quad 3x \equiv 4 \bmod 5 \quad\quad \Leftrightarrow \quad x \equiv 3 \bmod 7$$

Also gibt es 3 Lösungen:
$\forall y \in \mathbb{N} \mid 0 \leq y \leq 2 : x \equiv y \bmod 3$

$$\Leftrightarrow \quad x \equiv 3 \bmod 5$$

Die gemeinsamen Lösungen lasen sich jetzt mit dem Chinesischen Restsatz bestimmen:

$$b_1 = 5 \cdot 7 = 35$$
$$b_2 = 3 \cdot 7 = 21$$
$$b_3 = 5 \cdot 3 = 15$$

$$35x_1 \equiv 0 \bmod 3 \vee 35x_1 \equiv 1 \bmod 3 \vee 35x_1 \equiv 2 \bmod 3$$
$$\Leftrightarrow \quad x_1 \equiv 0 \bmod 3 \vee x_1 \equiv 1 \bmod 3 \vee x_1 \equiv 2 \bmod 3$$

$$21x_2 \equiv 3 \bmod 5$$
$$\Leftrightarrow \quad x_2 \equiv 3 \bmod 5$$

$$15x_3 = 3 \bmod 7$$
$$\Leftrightarrow \quad x_3 = 3 \bmod 7$$

$$x \equiv 21 \cdot 3 + 0 \cdot 35 + 3 \cdot 15 \equiv 108 \equiv 3 \bmod 105 \quad \vee$$
$$x \equiv 21 \cdot 3 + 1 \cdot 35 + 3 \cdot 15 \equiv 143 \equiv 38 \bmod 105 \quad \vee$$
$$x \equiv 21 \cdot 3 + 2 \cdot 35 + 3 \cdot 15 \equiv 178 \equiv 73 \bmod 105$$

$$L = \{3, 38, 73\}$$

(v)

$$x^2 + x + 4 \equiv 0 \bmod 19$$
$$\Leftrightarrow \quad x^2 + x + \left(2^{-1}\right)^2 - \left(2^{-1}\right) + 4 \equiv 0 \bmod 19$$
$$\Leftrightarrow \quad x^2 + x + 10^2 - 10^2 + 4 \equiv 0 \bmod 19$$
$$\Leftrightarrow \quad \left(x + 10\right)^2 - 10^2 + 4 \equiv 0 \bmod 19$$
$$\Leftrightarrow \quad \left(x + 10\right)^2 - 96 \equiv 0 \bmod 19$$
$$\Leftrightarrow \quad \left(x + 10\right)^2 \equiv 96 \bmod 19$$
$$\Leftrightarrow \quad \left(x + 10\right)^2 \equiv 1 \bmod 19$$
$$\Leftrightarrow \quad x + 10 \equiv 1 \bmod 19 \vee x + 10 \equiv 18 \bmod 19$$
$$\Leftrightarrow \quad x \equiv 10 \bmod 19 \vee x \equiv 8 \bmod 19$$

$$L = \{8, 10\}$$

(vi) Fine alle Lösungen von $x \equiv 2 \bmod 7$ und $x^2 \equiv 1 \bmod 11$

$x \equiv 2 \bmod 7$

$$x^2 \equiv 1 \bmod 11$$
$$\Leftrightarrow \quad x \equiv 1 \bmod 11 \vee x \equiv 10 \bmod 11$$

Die gemeinsamen Lösungen lassen sich mit den chinesischen Restsatz bestimmen:

$b_1 = 11$

$b_2 = 7$

$$11x_1 \equiv 2 \bmod 7$$
$$\Leftrightarrow \quad 4x_1 \equiv 2 \bmod 7$$
$$\Leftrightarrow \quad x_1 \equiv 2 \bmod 7$$

$$7x_2 \equiv 1 \bmod 11 \vee 7x_2 \equiv 10 \bmod 11$$
$$\Leftrightarrow \quad x_2 \equiv 8 \bmod 11 \vee x_2 \equiv 3 \bmod 11$$

$$x \equiv 11 \cdot 4 + 7 \cdot 8 \equiv 100 \equiv 23 \bmod 77 \qquad \vee$$
$$x \equiv 11 \cdot 4 + 7 \cdot 3 \equiv 65 \bmod 77$$

$$L = \{23, 65\}$$

Aufgabe 9.2

(i) $N = p \cdot q = 66\,013$

$\varphi(N) = (p-1) \cdot (q-1) = 65\,500$

(ii) $d = \frac{1}{e} \bmod \varphi(N) = \frac{1}{17} \bmod 65\,500 = 3\,853$

(iii)

Klartext	O	k
ASCII-Wert	79	107
Wert eines Paares	20 331	
Verschlüsselter Text ($y = x^e \bmod N$)	$20\,331^{17} \bmod 66\,013 = 3\,263$	

(iv)

Verschlüsselter Text (y)	$20\,331^{17} \bmod 66\,013 = 3\,263$	
Wert eines Paares entschlüsselt ($z = y^d \bmod N$)	$3\,263^{3\,853} \bmod 66\,013 = 20\,331$	
ASCII-Wert	79	107
Klartext	O	k

(v) Texte in Zahlen umwandeln und zurück

Text in Zahl

```
> txt2num := proc( txt )
  convert( txt, bytes ) mod 256;
  convert( %, base, 256, 256^nops(%) );
  %[1];
  end:
```

Zahl in Text

```
> num2txt := proc( n )
    convert( n, base, 256 );
    convert( %, bytes );
  end:
> x:=txt2num("Ok");
> p:=nextprime(200);
> q:=nextprime(300);
> if p=q then
        ERROR("p = q ist verboten!");
  else printf("Ok."); fi;
> N:=p*q;
> L:=(p-1)*(q-1);
> while igcd(e,L)<>1 do
     e:=rand(3..N-2)()
  end do;
> d:=1/e mod L;
> (d*e-1)/L;
  type( %, integer);
> p:='p';
  q:='q';
> L:='L';
> public := [N,e];
> secret := [N,d];
> y := x &^ e mod N;
> z := y &^d mod N;
> num2txt(z);
```

Aufgabe 9.3

(i)

n	prim	$2^{n-1} \operatorname{rem} n$	$2^{n-1} \equiv 1 \bmod n$
3	ja	1	ja
5	ja	1	ja
7	ja	1	ja
9	nein	4	nein
11	ja	1	ja
13	ja	1	ja
15	nein	1	ja
17	ja	1	ja
19	ja	1	ja
1105	nein	1	ja

(ii) (a) Die Gleichung $2^{n-1} \equiv 1 \bmod n$ gilt für $n = \{3,5,7,11,13,15,17,19,1105\}$.

(b) Die Zahlen $n = \{3,5,7,11,13,17,19\}$ sind prim.

Die Menge aus (b) ist eine Teilmenge der Menge aus (a).

(iii) $n \text{ prim} \Rightarrow 2^{n-1} \equiv 1 \bmod n$

Da n prim ist gilt $\varphi(n) = n-1$. Da 2 ebenfalls prim ist und n und 2 somit Teilerfremd sind, gilt nach LaGrange $2^{n-1} \equiv 1 \bmod n$.

(iv) $2^{n-1} \equiv 1 \bmod n \Rightarrow n$ prim gilt nicht, da $2^{n-1} \equiv 1 \bmod n$ für $n = 1105$ gilt, was aber nicht prim ist.

(v)
```
> for n from 3 to 1000 do
    Modulo:=evalb((2^(n-1) mod n)=1);
    if not evalb(Modulo = isprime(n)) then
        print(n);
    end if;
  end do:
```
Die Zahlen sind 341, 561, 645.

Aufgabe 9.4

(i) Sei $ab \equiv 0 \bmod p$. Zu zeigen: Dann ist auch $a \equiv 0 \bmod p$ oder $b \equiv 0 \bmod p$

$$ab \equiv 0 \bmod p$$
$$\Leftrightarrow \quad p \mid ab$$

Wenn p das Produkt zweier Zahlen teilt, muss p Primfaktor einer dieser Zahlen sein. Also teilt p eine dieser Zahlen, sodass entweder $a \equiv 0 \bmod p$ oder $b \equiv 0 \bmod p$.

(ii)
$$x^2 \equiv 1 \bmod p$$
$$\Leftrightarrow \quad x_{1/2} \equiv \pm 1 \bmod p$$

(iii)
$$x^2 \equiv 1 \bmod p$$
$$\Leftrightarrow \quad x^2 - 1 \equiv 0 \bmod p$$
$$\Leftrightarrow \quad (x-1)(x+1) \equiv 0 \bmod p$$

Nach i folgt daraus $x \equiv 1 \bmod p \vee x \equiv -1 \bmod p$

■

Aufgabe 9.5

(i) Zu zeigen: $\frac{p+1}{4}$ ist ganzzahlig

Da $p \equiv 3 \bmod 4$, ist $p+1$ ohne Rest durch 4 teilbar

(ii) Zu zeigen: $a^{p+1} \equiv a^2 \bmod p$

$$a^{p+1} \equiv a^2 \bmod p$$
$$\Leftrightarrow \quad a^2 \cdot a^{p-1} \equiv a^2 \bmod p$$

Nach Fermat gilt:

$$a^2 \cdot 1 \equiv a^2 \bmod p$$
$$\Leftrightarrow \quad a^2 \equiv a^2 \bmod p$$

■

(iii) Zu zeigen: $a^{\frac{p+1}{2}} \equiv \pm a \bmod p$

$$a^{\frac{p+1}{2}} \equiv \pm a \bmod p$$
$$\Leftrightarrow \quad a^{p+1} \equiv a^2 \bmod p$$

Dies gilt nach ii. Nach 9.4 ii und iii gibt es nur diese beiden Lösungen.

■

(iv) Sei $b = a^2$ und $w = b^{\frac{p+1}{4}}$. Zu zeigen: $a \equiv \pm w \bmod p$

$$a \equiv \pm w \bmod p$$

$$\Rightarrow \quad a \equiv \pm b^{\frac{p+1}{4}} \bmod p$$

$$\Rightarrow \quad a \equiv \pm \left(a^2\right)^{\frac{p+1}{4}} \bmod p$$

$$\Leftrightarrow \quad a \equiv \pm a^{\frac{2(p+1)}{4}} \bmod p$$

$$\Leftrightarrow \quad a \equiv \pm a^{\frac{p+1}{2}} \bmod p$$

$$\Leftrightarrow \quad \pm a \equiv a^{\frac{p+1}{2}} \bmod p$$

Dies gilt nach iii.

■