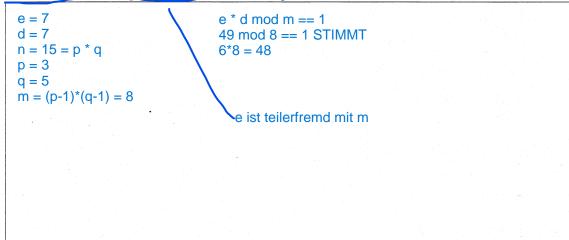
## Aufgabe 2: RSA

[14 Punkte]

Betrachten Sie RSA mit öffentlichen Schlüssel P=(7,15) und geheimen Schlüssel S=(7,15).

(a) [6 Punkte] Ist das gegebene Schlüsselpaar mathematisch korrekt? Welche notwendigen mathematischen Eigenschaften werden eingehalten?



(b) [2 *Punkte*] Ist die Wahl dieser Schlüsselpaare für den praktischen Einsatz sinnvoll? Begründen Sie Ihre Antwort mit einem Satz.

NEIN, weil die zwei Schlüssel gleich sind.

(c) [6 Punkte] Verschlüsseln Sie die Zahl 2 ohne ein Zwischenergebnis größer als 100 zu verwenden. Geben Sie die Berechnungsschritte an!

```
2^7 = 2 * 2^6
Ö:
                                          (e, n)
Geheime Nachricht = (Originelle Nachricht)^e mod n
         15 = (2 * 2^6) mod 15 = (2 mod 15) * (64 mod 15) = 2 * 4 = 8
       P: (d, n)
      (7, 15)
P:
                                             (d, n)
       Entschlüsselte Nachricht = (Geheime)^d mod n
       = 8^7 \mod 15 = 2
```