The function \( \phi \) in RSA key generation is a **counting function**. There are a few well-known counting functions and are defined as follows.

\[
\begin{align*}
\tau(n) &= \text{number of divisors of } n \\
\sigma(n) &= \text{sum of divisors of } n \\
\phi(n) &= \text{number of positive integers not exceeding } n \text{ that are coprime to } n
\end{align*}
\]

For example, the divisors of 12 are 1, 2, 3, 4, 6, 12 and the numbers that are coprime to 12 are 1, 5, 7, 11. Therefore,

\[
\begin{align*}
\tau(12) &= 6 \\
\sigma(12) &= 28 \\
\phi(12) &= 4
\end{align*}
\]

**1)** Find the \( \tau, \sigma, \phi \) values for the following integers

(a) 18  
(b) 36  
(c) 47  
(d) 48  
(e) 128  
(f) 144  
(g) 2 \cdot 3 \cdot 5 \cdot 7  
(h) 2^{12}  
(i) 2^3 \cdot 3^4 \cdot 5^7

**2)** Let \( p \) be a prime, what are the values of \( \tau(p), \sigma(p) \) and \( \phi(p) \)?

**3)** If \( n \geq 2 \), what is the minimum value for \( \tau(n) \)? What about maximum value? Use your calculator to generate some values of \( \tau(n) \) and give a conjecture. Can you argue why they are true?

**4)** Can you repeat the previous part and argue the same for \( \sigma(n) \)? What about \( \phi(n) \)?

**5)** If the factorization of \( n \) is known, then there are formulas for \( \tau(n), \sigma(n) \) and \( \phi(n) \). Find the formulas.

**6)** Suppose you do not know the factorization of \( n \), but you know \( \phi(n) \), would that compromise the security?

**7)** The generalized version of Fermat’s Little Theorem is the Euler-Fermat Theorem. Let \( n \geq 2 \) be an integer and \( \gcd(m, n) = 1 \), then

\[
m^{\phi(n)} \equiv 1 \pmod{n}.
\]

Use this theorem to show that when \( c \equiv m^e \pmod{n} \) and \( m' \equiv c^d \pmod{n} \), then \( m \equiv m' \pmod{n} \). (This is to verify that the RSA algorithm does work.)

**8)** Extend the RSA encryption to a product of three primes \( n = pqr \). What has to be changed in the algorithm? Can you extend this further? What do you think of the security and the practicality in these extensions?