[P11] (RSA public key cryptography). We need two results that will be presented in the lecture: The first is Euclid's algorithm as indicated on the previous sheet. The second fact is as follows: let $\phi(n)$ be the number of integers in $[1, n-1]$ which are co-prime to n (the function ϕ is *Euler's totient function*). Then if a is co-prime to n, then $a^{\phi(n)} = 1 \pmod n$.

To send a secrete message from Bob to Alice, the parties perform the following protocol:

1. Alice creates two large random prime numbers p, q. Let $n = pq$.
2. Alice chooses a random integer e that is relatively prime to n. She computes the multiplicative inverse d of e modulo $\phi(n)$ (Euclid's algorithm). Alice publicly announces the pair (e, n) (the *public key*).
3. Suppose now Bob wants to send a message, m, to Alice. Assume that m is a number smaller than n (if not, break its binary representation into pieces of $\log_2 n$ bits each and encode every piece separately). Bob computes $m^e \pmod n$ and publicly announces it.
4. Alice computes $(m^e)^d \pmod n$.

In this exercise, we will prove that Alice recovers the message by Bob. A third observer, Eve, is assumed to have access to all communications between Alice and Bob (i.e. to e, n, and $m^e \pmod n$). We will argue that it is probably difficult for Eve to learn m, unless she operates a quantum computer.

(1) What is $\phi(n)$? Why is there an efficient way for Alice to compute $\phi(n)$ ("efficient" means polynomial in the number of bits of n)? Convince yourself that there is no *obvious* efficient way for Bob and Eve to do the same (no written answer needed here, of course).

(2) Assume for the moment that m is co-prime to n. Show that $(m^e)^d = m \pmod n$, so that Alice recovers the message in this case. (Hint: use the "second fact" provided above).

(3) The remaining case makes use of the (reverse direction of the) *Chinese Remainder Theorem*: if $x = m \pmod p$ and $x = m \pmod q$ then $x = m \pmod{pq}$. Prove that. (Hint: show that if m' is some number fulfilling the first two equations, then it it differs from m only by a multiple of pq).

(4) Now assume that m and n are not co-prime. Show that in this case, m is divisible by either p or q, but not by both. Without loss of generality, assume that p divides n. Prove that $m^{ed} = 0 \pmod p$ and $m^{ed} = m \pmod q$ (use Fermat's Little Theorem). Now use (3) to establish that also in this case, $(m^e)^d = m \pmod n$.

(5) Show that if Eve could compute prime factorizations efficiently (which quantum computers can), she could efficiently compute d and hence break the cryptosystem. There is a different attack Eve could mount with the help of a quantum computer. As we will see shortly, quantum mechanics allows us to solve the *order finding problem* efficiently: Assume that a function f is periodic, in that there exists a number r such that $f(x) = f(x+r)$ for all x. The order finding problem is to find r from f. Assume Eve could solve the order finding problem for the function $f(x) = (m^e)^x \pmod n$. Assume further that e is co-prime to the solution r (this is always true, as a consequence of *Lagrange's Theorem*, but we won't show that here). Let d' be the multiplicative inverse of e modulo r. Show that $(m^e)^{d'} = m \pmod n$. (Hint: use $f(r) = f(0)$). (10)