

- (1) Give a careful proof by induction that Euclidean algorithm always allows to express (a, b) as $(a, b) = ax + by$ for some integer x, y .
Hint: Use induction in the number of steps in the Euclidean algorithm.
- (2) Prove that the equation $ax + by = c$ has integer solutions if and only if $(a, b) | c$.
- (3) Without using the uniqueness of prime factorization theorem prove that if $a|m$, $b|m$ and $(a, b) = 1$ then $ab|m$.
- (4) Let a, b be integers. Suppose $ax_0 + by_0 = (a, b)$ where x_0, y_0 are provided by the Euclidean algorithm.
 - (a) Suppose $(a, b) = 1$. Find all integer solutions of $ax + by = (a, b)$
 - (b) Find all integer solutions of $ax + by = (a, b)$ in general (i.e without assuming that $(a, b) = 1$).
 - (c) Find all integer solutions of $16x + 6y = (16, 6)$.
- (5) Carry out all the steps of RSA encryption algorithm and verify the results for
 $p = 7, q = 5, e = 11$ and message $M = 31$.