Assignment I

Computational Algebra

1. Recall that the extended Euclid's algorithm on input polynomials $r_0 = f(x)$ and $r_1 = g(x)$ finds r_i, s_i, t_i for each iteration until the last iterations gives $r_l = \gcd(f,g)$ satisfying $r_l = s_l f + t_l g$. Prove the following for all values $0 \leq i \leq l$.
   1. $GCD(f,g) = GCD(r_i, r_{i+1}) = r_l$.
   2. $s_i f + t_i g = r_i$
   3. $s_i t_{i+1} - t_i s_{i+1} = (-1)^i$
   4. $GCD(r_i, t_i) = GCD(f, t_i)$.
   5. $f = (-1)^i (t_{i+1} r_i - t_i r_{i+1})$.
   6. $g = (-1)^i (s_{i+1} r_i - s_i r_{i+1})$

2. Compute s_i, t_i and r_i for each value of i for rational polynomials $f(x) = x^3 + 6x^2 + 11x + 6$ and $g(x) = x^2 - 1$. What is the value of l for this case?

3. Suppose a, n are positive integers, $1 \leq a \leq n$. Let $d = \gcd(a,n)$. Suppose b is a multiple of d. Show that:
   - The equation $ax = b \mod n$ is solvable.
   - If x is one solution, $x + \frac{n}{d}$ is also a solution.
   - The equation has exactly d solutions between 1 and n.
   - For what values of a between 1 and 20 does the equation $ax = 12 \mod 20$ fail to have a solution?

4. Let F be a finite field. Let p the least postive integer such that $1 + 1 + ..1$ (p times) gives 0. Show that p is prime. p is called the **characteristic** of the field F.

5. A real number α is a repeated root of a real polynomial $f(x)$ if $(x-\alpha)^2$ divides $f(x)$. Show that in $\mathbf{C[x]}$, f has a repeated root if only if $GCD(f, f') \neq 1$ (where f' refers to the derivative of f).

6. Let a, b be (given) positive integers.
   1. For a given positive integer n, show that $a^n \mod n$ can be computed in $O(\log n)$ multiplications.
   2. Given only b, show that the problem of finding a and n such that $b = a^n$ for some positive integer n (if one such (a,n) pair exists) is computable with $O(\log^2 b)$ multiplications.

7. Let F be a field. Show that the ring $F[x]/p(x)$ is a field if and only if $p(x)$ is an irreducible polynomial.

8. An element $a \in \mathbf{Z}_n$ such that $a \notin \{\pm 1\} \mod n$ but $a^2 = 1$ is called a non-trivial square root of unity in $\mathbf{Z}_n$ Let $n = p_1 p_2 p_3 ... p_k$, where $p_1 .., p_k$ are distinct odd prime numbers.
   1. Show that the equation $x^2 - 1 \mod n$ has 2^k distinct solutions in $\mathbf{Z}_n$. (Hint: Use Chinese remainder theorem)
   2. Suppose you know the value of one non-trivial square root of unity, show that you can find out a non-trivial divisor of n.

9. Suppose F be a field with m elements. Show that every element $\alpha \in F$ is a root of the polynomial $x^m - x$. Use this fact to show that the product of all non-zero elements in F must be -1. (In particular, it follows that $1.2.3...(p-1) \equiv -1 \mod p$, a result known as Wilson's Theorem). .

10. An ideal I in a ring R is maximal if there is no ideal in R that is a strict superset of I other than the whole R itself. Show that if I is a maximal ideal, then R/I is a field.