1. (i) Carefully state Fermat’s theorem. (ii) Show that \( n^{13} - n \) is divisible by 2, 3, 5, 7, and 13 for any \( n \).

2. (i) What is the order of \( U_{15} \), the group of units mod 15? (ii) What is the order of [2] in \( U_{15} \)? (iii) Find all the cosets of the subgroup generated by [2]. (iv) How does this illustrate Lagrange’s Theorem?

3. (i) If \( G \) is a group with operation \( \circ \) and \( H \) is a group with operation \( * \), define what a homomorphism from \( G \) to \( H \) is. (ii) Which homomorphisms are isomorphisms? (iii) Find a one-to-one homomorphism \( f \) from \( U_{12} \) to the symmetric group \( S_4 \). (iv) Is \( f \) an isomorphism?

4. Let \( f(x) = x^4 + x^2 + 1 \) and \( g(x) = x^3 + 1 \) in \( \mathbb{Z}/2\mathbb{Z}[x] \). (i) Find a greatest common divisor \( d(x) \) of \( f(x) \) and \( g(x) \). (ii) Find polynomials \( r(x) \) and \( s(x) \) such that

\[
d(x) = r(x)f(x) + s(x)g(x)
\]

(iii) Factor \( f(x) \) into a product of irreducible polynomials.
(1)(i) If $a$ is an integer not divisible by the prime $p$, then $a^{p-1} \equiv 1 \pmod{p}$.
(ii) $n^{13} - n = n(n^{12} - 1)$ and so we must show that for $p = 2, 3, 5, 7, 13$, $n \equiv 0 \pmod{p}$ or $n^{12} \equiv 1 \pmod{p}$. By Fermat, if $n \not\equiv 0 \pmod{p}$, then $n^{p-1} \equiv 1 \pmod{p}$. In each case, $p - 1$ divides 12 and so $n^{12} \equiv 1 \pmod{p}$.

(2)(i) The order of $U_{15}$ is $\phi(15) = \phi(3)\phi(5) = 8$.
(ii) Powers of 2 (mod 15) are 2, 4, 8, 1 and so the order of [2] is 4.
(iii) The subgroup generated by [2] is {[2], [4], [8], [1]}, leaving {[7], [11], [13], [14]} to make up the other coset.
(iv) The number of cosets (2) equals the order of $U_{15}$ (8) divided by the order of the subgroup (4).

(3)(i) A homomorphism is a function $f : G \rightarrow H$ such that $f(a \circ b) = f(a) \ast f(b)$ for all $a, b$ in $G$ and $f(e) = e'$ if $e, e'$ are the identity elements of $G, H$.
(ii) An isomorphism is a homomorphism that is one-to-one and onto.
(iii) Multiplication by [1], [5], [7], [11], which make up $U_{12}$, sends the elements to 1, 5, 7, 11; 5, 1, 11, 7; 7, 11, 1, 5; 11, 7, 5, 1 respectively. Renaming the elements 1, 2, 3, 4 we see that $f$ maps [1], [5], [7], [11] to (1, 2, 3, 4), (2, 1, 4, 3), (3, 4, 1, 2), (4, 3, 2, 1) respectively.
(iv) No, since not onto ($S_4$ has 4! = 24 elements).

(4)(i) $x^4 + x^2 + 1 = x(x^3 + 1) + (x^2 + x + 1)$. $x^3 + 1 = (x + 1)(x^2 + x + 1) + 0$. Thus a gcd is $x^2 + x + 1$.
(ii) $x^2 + x + 1 = (x^4 + x^2 + 1) - x(x^3 + 1)$, so $r(x) = 1, s(x) = -x(\equiv x)$.
(iii) By (i), $x^2+x+1$ divides $f(x)$. The quotient is $x^2+x+1$ so $f(x) = (x^2+x+1)^2$, and $x^2 + x + 1$ is irreducible since it has no linear factor since it has no root in $\mathbb{Z}/2\mathbb{Z}$. 