First part, questions 1 to 8

1. (a) Let $\mathbb{F}_5$ be the field of 5 elements. Find a greatest common divisor $d(X)$ of the polynomials

$$f(X) = X^5 + 2X^4 - X - 2 \qquad \text{and} \qquad g(X) = X^3 + X^2 + 3$$

in the ring $\mathbb{F}_5[X]$. (Provide the details of your computation.)

(b) If $d(X)$ is not monic, find the unique monic greatest common divisor $t(X)$ of $f(X)$ and $g(X)$.

(c) Find $r(X), s(X) \in \mathbb{F}_5[X]$ such that $f(X)r(X) + g(X)s(X) = t(X)$.

[**6 points**]

Solution:

(a)

$$\begin{array}{l|l}
X^5+2X^4-X-2 & X^3+X^2+3 \\ \hline
-\left(X^5+X^4+3X^2\right) & X^2+X-1 \\
X^4-3X^2-X-2 & \\
-\left(X^4+X^3+3X\right) & \\
-X^3-3X^2-4X-2 & \\
-\left(-X^3-X^2-3\right) & \\
-2X^2-4X+1 &
\end{array}
\qquad
\begin{array}{l|l}
X^3+X^2+3 & -2X^2-4X+1 \\ \hline
-\left(X^3+2X^2-3X\right) & -3X+3 \\
-X^2+3X+3 & \\
-\left(-X^2-2X+3\right) & \\
0 &
\end{array}$$

$$\gcd(f(X),g(X)) = \boxed{-2X^2-4X+1 = 3X^2+X+1} = 3(X^2+2X+2)$$

(b) $3X^2+X+1 = 3(X^2+2X+2) \Rightarrow$ monic $\gcd(f,g) = \boxed{t(X) = X^2+2X+2}$

(c) $3X^2+X+1 = f(X) - (X^2+X-1)g(X) = 3t(X)$

$$\Rightarrow t(X) = \frac{1}{3}f(X) - \frac{1}{3}(X^2+X-1)g(X) =$$

$$= \boxed{2f(X) - (2X^2+2X-2)g(X) = t(X)}$$

$\boxed{r(X) = 2}$, $\boxed{s(X) = -2X^2-2X+2}$

2. (a) Let G be a finite group. Recall that the center of a group $Z(G)$ is the set of all elements $z \in G$ such that $zg = gz$ for any $g \in G$. Show that $Z(G)$ is a subgroup in G.

(b) Fix an element $x \in G$. Recall that the centralizer $H \subset G$ of an element $x \in G$ is the set of all elements $h \in G$ such that $hx = xh$. Show that H is a subgroup of G, and that $Z(G)$ is a subgroup of H: $Z(G) \subset H \subset G$.

(c) Let $|G| = 9$. Show that $|Z(G)| \geq 3$. *Hint:* Recall the class equation of G: $|G| = |Z(G)| + \sum_i [G : H_i]$, where H_i are the stabilizers of representatives of the nontrivial conjugacy classes in G.

centralizers

(d) Let $|G| = 9$. Fix an element $x \in G$ and let H be the centralizer of x in G. Use (b) and (c) to show that $|H| \geq 4$.

(e) Derive from (d) that any group of order 9 is abelian.

(f) Let $|G| = p^2$, where p is a prime. Generalize (c), (d), (e) to show that a group of order p^2 is abelian.

[14 **points**]

Solution: (a) $1 \in G$, $1g = g1 \Rightarrow 1 \in Z(G)$

If $g_1, g_2 \in Z(G) \Rightarrow g_1 g_2 z = g_1 z g_2 = z g_1 g_2 \Rightarrow g_1 g_2 \in Z(G)$

If $g \in Z(G) \Rightarrow zg = gz \Rightarrow zgg^{-1} = gzg^{-1} \Rightarrow g^{-1}gzg^{-1} = g^{-1}gzg^{-1}$

$\Rightarrow g^{-1}z = zg^{-1}$

$\Rightarrow g^{-1} \in Z(G) \Rightarrow Z(G)$ is a subgroup in G.

(b) Let $x \in G$. If $h_1, h_2 \in H_x \Rightarrow h_1 h_2 x = h_1 x h_2 = x h_1 h_2 \Rightarrow h_1 h_2 \in H_x$

$1x = x1 \Rightarrow 1 \in H_x$

If $h \in H_x \Rightarrow hx = xh \Rightarrow x = h^{-1}xh \Rightarrow xh^{-1} = h^{-1}x \Rightarrow h^{-1} \in H_x$

$\Rightarrow H_x \subset G$ is a subgroup in G.

Also, if $z \in Z(G) \Rightarrow zx = xz \Rightarrow Z(G) \subset H_x \subset G$ subgroups.

(c) $|G| = 9$. We have the classe equation:

$$|G| = |Z(G)| + \sum_{\substack{i \\ \text{nontrivial conj classes in } G}} |C_i| = |Z(G)| + \sum_i [G : H_i]$$

centralizer of representatives of nontrivial conj. classes.

Since $Z(G) \subset G$ and $H_i \subset G$ are subgroups

$\Rightarrow$ By Lagrange's theorem $|Z(G)|$ divides $|G|$

$|H_i|$ divides $|G|$ $\Rightarrow [G : H_i] = |G|/|H_i|$ divides $|G|$

$\Rightarrow$ ~~since~~ $|C_i| = [G : H_i] > 1$ by definition of nontrivial conj class

$\Rightarrow 3$ divides $|C_i|$ $\forall i$

$\Rightarrow \underset{3|}{|G|} = |Z(G)| + \underbrace{\sum_i |C_i|}_{3|} \Rightarrow 3$ divides $|Z(G)|$

$\Rightarrow |Z(G)| \geq 3$

(d) $|G| = 9$. Let $x \in G$ and H_x be the centralizer of x in G

$\Rightarrow$ by (b) $Z(G) \subset H_x \Rightarrow$ if $x \notin Z(G) \Rightarrow |H_x| \geq 4$

$x \cdot x = x \cdot x \Rightarrow x \in H_x \Rightarrow$ if $x \in Z(G) \Rightarrow H_x = G \Rightarrow |H_x| = |G| = 9$

(e) We have $[G : H_i] = |G|/|H_i|$ is a multiple of 3 by (c)

and $|H_i| \geq 4$ by (d) $\Rightarrow |H_i| = 9$ since $H_i \subset G$ is a subgroup,

but $|C_i| = |G|/|H_i| > 1$ by definition $\Rightarrow$ no nontrivial conjugacy classes exist in G $\Rightarrow |G| = |Z(G)|$ and $G = Z(G)$ is an abelian group.

(d) If $|G| = p^2$ $\Rightarrow \underset{p|}{|G|} = |Z(G)| + \underbrace{\sum [G : H_i]}_{p|} \Rightarrow p$ divides $|Z(G)|$

p a prime

$Z(G) \subset H_i$

$x \subset H_i$, where x is a representative of the nontrivial conj class C_i

$\Rightarrow |H_i| \geq p+1 \Rightarrow |H_i| = p^2$ since $H_i \subset G$ is a subgroup

but $|G|/|H_i| = |C_i| > 1$ by def $\Rightarrow$ no nontrivial conj classes can exist in G

$\Rightarrow G = Z(G)$ is abelian.

3. (a) Define the Euler totient function $\varphi(n)$ for a natural $n \geq 2$ and state the Euler theorem about congruences.

(b) Let p_1, p_2, p_3 be three primes, not necessarily distinct. Express $\varphi(p_1p_2p_3)$ in terms of p_1, p_2, p_3. Consider cases.

(c) Show that $a = p^{88} - p^{16}$ is divisible by 30 for any prime $p \geq 7$.

[10 **points**]

Solution: (a) $\varphi(n)$ is defined as the number of integers k such that $1 \leq k \leq n$ and k is coprime with n. $(\gcd(k,n)=1)$

Thm (Euler): Let $a, n \in \mathbb{Z}^+$, $\gcd(a,n)=1$.

Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

(b) If $\gcd(m,n)=1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$; $\varphi(p^k) = p^k - p^{k-1}$

If p_1, p_2, p_3 are three distinct primes $\Rightarrow \varphi(p_1p_2p_3) = \varphi(p_1)\varphi(p_2)\varphi(p_3) =$
$= \boxed{(p_1-1)(p_2-1)(p_3-1)}$

If $p = p_1 = p_2$ and $p_3 \neq p \Rightarrow \varphi(p_1p_2p_3) = \varphi(p^2p_3) = \varphi(p^2)\varphi(p_3) = \boxed{(p^2-p)(p_3-1)}$

If $p = p_1 = p_2 = p_3 \Rightarrow \varphi(p_1p_2p_3) = \varphi(p^3) = \boxed{p^3 - p^2}$

(c) Let $p \geq 7$ a prime $\Rightarrow p$ is coprime with 2, 3 and 5

$\Rightarrow \gcd(p, 30) = 1 \Rightarrow$ by Euler's thm $p^{\varphi(30)} \equiv 1 \pmod{30}$

$\varphi(30) = \varphi(2 \cdot 3 \cdot 5) = (2-1)(3-1)(5-1) = 8$

$\Rightarrow p^8 \equiv 1 \pmod{30} \Rightarrow p^{88} = (p^8)^{11} \equiv 1 \pmod{30}$

$p^{16} = (p^8)^2 \equiv 1 \pmod{30}$

$\Rightarrow \boxed{p^{88} - p^{16} \equiv 0 \pmod{30}}$

4. Let C_k denote the cyclic group of order $k \in \mathbb{N}^+$.

(a) How many different (non-isomorphic) abelian groups of order 144 are there? List the elementary divisors and invariant factors for each of the groups.

(b) Let m_G be the maximal order of an element in G. Among the groups listed in (a), find the one where m_G is the smallest. Justify your answer.

(c) Among the groups listed in (a), find all groups of the form $H \times K$ where $|H| = |K| = 12$. Justify your answer.

[9 **points**]

Solution: (a) $|G| = 144 = 2^4 \cdot 3^2$

partitions of 4: (4), (3,1), (2,2), (2,1,1), (1,1,1,1)

partitions of 2: (2), (1,1)

Possible abelian groups of order 144 up to isomorphism: $\boxed{10}$

$C_{16} \times C_9$ $\quad$ C_{144}

$C_8 \times C_2 \times C_9$ $\quad$ $C_{72} \times C_2$

$C_4 \times C_4 \times C_9$ $\quad$ $C_{36} \times C_4$

$C_4 \times C_2 \times C_2 \times C_9$ $\quad$ $C_{36} \times C_2 \times C_2$

$C_2 \times C_2 \times C_2 \times C_2 \times C_9$ $\quad$ $C_{18} \times C_2 \times C_2 \times C_2$

$C_{16} \times C_3 \times C_3$ $\quad$ $C_{48} \times C_3$

$C_8 \times C_2 \times C_3 \times C_3$ $\quad$ $C_{24} \times C_6$

$C_4 \times C_4 \times C_3 \times C_3$ $\quad$ $C_{12} \times C_{12}$

$C_4 \times C_2 \times C_2 \times C_3 \times C_3$ $\quad$ $C_{12} \times C_6 \times C_2$

$C_2 \times C_2 \times C_2 \times C_2 \times C_3 \times C_3$ $\quad$ $C_6 \times C_6 \times C_2 \times C_2$

Elementary divisors:

(16,9) (8,2,9), (4,4,9), (4,2,2,9), (2,2,2,2,9), (16,3,3), (8,2,3,3) (4,2,2,3,3) (2,2,2,2,3,3),

Invariant factors:

(144), (72,2), (36,4), (36,2,2), (18,2,2,2), (48,3), (24,6), (12,12), (12,6,2) (6,6,2,2),

(b) If $(d_1, d_2 \ldots d_n)$ are the invariant factors of an abelian group, where $d_n | d_{n-1} \ldots d_2 | d_1$ => $C_{d_1} \times C_{d_2} \times \ldots \times C_{d_n}$

If $t = (t_1, t_2 \ldots t_n) \in C_{d_1} \times C_{d_2} \times \ldots \times C_{d_n}$ => $\text{order}(t) = \text{lcm}(d_1, d_2 \ldots d_n) = d_1$

=> The maximal possible order m_G of an elt in G is the smallest if d_1 is the smallest => The group among the listed in (a) where m_G is the smallest is $\boxed{C_6 \times C_6 \times C_2 \times C_2}$ $(d_1 = 6)$, and $m_G = 6$.

(c) $G = H \times K$ s.t. $|H| = |K| = 12$ => G cannot have C_{2^k} with $k \geq 3$ and C_{3^m} with $m \geq 2$ in the decomposition into the elementary divisors

=> There are just 3 such groups: $C_4 \times C_4 \times C_3 \times C_3 = \boxed{\underbrace{C_{12}}_{H} \times \underbrace{C_{12}}_{K}}$

$C_4 \times C_2 \times C_2 \times C_3 \times C_3 = \boxed{\underbrace{C_{12}}_{H} \times \underbrace{(C_6 \times C_2)}_{K}}$

$C_2 \times C_2 \times C_2 \times C_2 \times C_3 \times C_3 = \boxed{\underbrace{(C_6 \times C_2)}_{H} \times \underbrace{(C_6 \times C_2)}_{K}}$

5. Let $\mathbb{F}_3$ be the field of 3 elements. Define the ideal in $\mathbb{F}_3[X]$

$$I = \langle X^2 - X - 1 \rangle$$

Let

$$A = \mathbb{F}_3[X]/I$$

(a) Show that A is a field. Justify your answer (cite a theorem from the course).

(b) List all elements in A.

(c) Consider the group of units (invertible elements) A^* in A. List all elements in A^*. Find the order and structure of A^* (cite a theorem from the course).

(d) Find all elements of the multiplicative order 2 in the group of units A^*.

(e) Does A^* have an element of order 8? If so, give an example of such an element.

[12 **points**]

Solution: (a) $f(x) = X^2 - X - 1$ is a polynomial of degree 2 with no roots in $\mathbb{F}_3$: $f(0) = -1$, $f(1) = -1$, $f(-1) = 1$.

$\Rightarrow$ $f(X)$ is irreducible. By the theorem from the course,

$A = \mathbb{F}_3[X]/\langle f(X)\rangle$ is a field $\Leftrightarrow$ $f(X)$ is irreducible over $\mathbb{F}_3$.

$\Rightarrow$ A is a field.

(b) Since $f(X)$ has degree 2, we have $3^2 = \boxed{9}$ elements in the field A:

$\{[0], [1], [-1], [X], [-X], [X-1], [X+1], [-X-1], [-X+1]\}$

(all polynomials in $\mathbb{F}_3[X]$ up to order 1).

(c) By the theorem from the course, for a finite field A,

$|A^*| = |A| - 1$ and A^* is a cyclic group.

In our case $A^* \simeq C_8 = \{[1], [-1], [X], [-X], [X-1], [X+1], [-X-1], [-X+1]\}$

(all nonzero elements in A).

(d) Since $C_8 = \{t, t^2, t^3, t^4, t^5, t^6, t^7, t^8 = 1\}$,

for an element α to have order 2, we need $\alpha = t^{4k}$ for some $k \in \mathbb{Z}$, k odd

(otherwise $\alpha = t^{8m} = 1$ has order 1)

There exist only one such element $\alpha = t^4$.

Looking at the list of elements of A, we immediately find $\boxed{\alpha = -1}$ of order 2.

(e) Since $A^* \simeq C^8$, it has elements of order 8 that generate the group. For example, $\beta = X$ has order 8:

$\beta^2 = X^2 = X + 1$, $\beta^3 = X(X+1) = X^2 + X = 2X + 1 = -X + 1$

$\beta^4 = X(-X+1) = -X^2 + X = -X - 1 + X = -1 = \alpha \Rightarrow \beta^8 = 1$.

(Also, $-X$, $-X+1$, $X-1$ have order 8 in A^*)

6. (a) Show that the system of congruences

$$\begin{cases} x \equiv 14 \pmod{20} \\ x \equiv 1 \pmod{3} \\ x \equiv 0 \pmod{11}. \end{cases}$$

has infinitely many solutions in $\mathbb{Z}$.

(b) Find all integer solutions of the system.

(c) Find the smallest positive integer that solves the system in (a).

[6 **points**]

Solution: (a) The integers $\{3, 11, 20\}$ are pairwise coprime. Therefore by the Chinese Remainder Theorem, there exist infinitely many solutions of the given system of the form $\{d + 660k\}_{k\in\mathbb{Z}}$

(b) $11t = 3s + 1$

$11t - 3s = 1$ $\Rightarrow$ $x \equiv 55 \pmod{33}$

$\Rightarrow$ $55 - 3\cdot 18 = 1$

$\begin{cases} x \equiv 22 \pmod{33} \\ x \equiv 14 \pmod{20} \end{cases}$ $\Rightarrow 33t + 22 = 20s + 14$

find solution by Euclidean division

$33 = 20\cdot 1 + 13$, $20 = 13\cdot 1 + 7$, $13 = 7\cdot 1 + 6$, $7 = 6\cdot 1 + 1$

$\Rightarrow 1 = 7 - 6 = 7 - (13 - 7) = (20 - 13) - 13 + (20 - 13) = 2\cdot 20 - 3\cdot 13 =$

$= 2\cdot 20 - 3(33 - 20) = 5\cdot 20 - 3\cdot 33.$

$\Rightarrow -40\cdot 20 + 24\cdot 33 = -8 \Rightarrow 33\cdot 24 + 22 = 814.$

$\Rightarrow \boxed{x = \{814 + k\cdot 660\}_{k\in\mathbb{Z}}}$

(c) $a = 814 - 660 = \boxed{154}$ is the smallest positive solution of the system.

7. Let S_n denote the symmetric group of permutations of $n \in \mathbb{N}^+$ elements.

(a) Consider the element $a = (1234567)(38) \in S_9$ and write it as a product of disjoint cycles. Find the order of a.

(b) Consider the element $b = (1234567)(25) \in S_9$ and write it as a product of disjoint cycles. Find the order of b.

(c) Let $2 \le k < n$ and consider the element $c = (12\ldots k)(im) \in S_n$ where $1 \le i \le k$ and $k < m \le n$. Write c as a product of disjoint cycles in S_n. Find the order of c as it depends on k.

(d) Let $2 \le k \le n$ and consider the element $d = (12\ldots k)(ij) \in S_n$ where $1 \le i < j \le k$. Write c as a product of disjoint cycles in S_n. Express the order of d in terms of i, j, k.

(e) Let $4 \le k+2 \le n$ and $k < i < j \le n$. Find the order of the element $e = (12\ldots k)(ij)$ as it depends on k.

(f) If an element is a product of a k-cycle and a 2-cycle (not necessarily disjoint) in a symmetric group, what can be the disjoint cycle decomposition of such an element? Use (c), (d), (e) to formulate a general statement.

[14 **points**]

Solution (a): $(1234567)(38) = (12384567)$ order$(a) = 8$

(b) $b = (1234567)(25) = (1267)(345)$ order$(b) = \mathrm{lcm}(4,3) = 12$

(c) $c = (12\ldots i{-}1\; i\; i{+}1 \ldots k)(im) = (12\ldots i\, m\; i{+}1 \ldots k)$ order$(c) = k+1$

(d) $d = (12\ldots i \ldots j \ldots k)(ij) = (12\ldots i\; j{+}1 \ldots k)(i{+}1 \ldots j)$ order$(d) =$

$= \mathrm{lcm}((j-i), (k-j+i))$.

(e) ~~There are 3 cases: odd~~ $k < i < j \le n$

$\Rightarrow e = (12\ldots k)(ij)$ is a product of disjoint cycles

$\Rightarrow$ order$(e) = \mathrm{lcm}(k, 2) = \begin{cases} k, & k \text{ is even} \\ 2k, & k \text{ is odd} \end{cases}$

(f) There are 3 cases:

(1) k-cycle is disjoint from 2-cycle $\Rightarrow$ cycle type is $(k, 2)$ (case (e)).

(2) 1 of the elements of the 2-cycle appears in the k-cycle, the other doesn't $\Rightarrow$ cycle type $(k+1)$ (case (c))

(3) Both elements of the 2-cycle appear in the k-cycle

$\Rightarrow$ cycle type $((k-j+i), (j-i))$ where $1 \le i < j \le k$ (case (d))

8. (a) State the definition of the characteristic of a ring.

(b) Let A and B be two rings of characteristics $c_A > 0$ and $c_B > 0$. Express the characteristic of the direct product $A \times B$ in terms of c_A, c_B.

(c) Suppose that $\gcd(n, m) = d \neq 1$ for integers $n > 1, m > 1$. Show that the rings $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/nm\mathbb{Z}$ are not isomorphic. *Hint:* use the characteristic of a ring.

(d) Find the number of units (invertible elements) in rings $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ and in $\mathbb{Z}/108\mathbb{Z}$. Justify your answer,

(e) Show that if $\gcd(n, m) > 1$, then the rings $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/nm\mathbb{Z}$ have different number of units.

[10 **points**]

Solution: (a) Let $1 \in A$. The smallest positive integer n s.t. $n \cdot 1 = 0$ in A is the characteristic of the ring A. If no such n exists, the characteristic of A is 0. (Alternatively, there exists a unique ring homomorphism $\varphi: \mathbb{Z} \to A$ with kernel $\ker \varphi = (d)$, then $d = \operatorname{char} A$).

(b) Let $n = \operatorname{char} A > 0$, $m = \operatorname{char} B > 0$. If $k \cdot (1,1) = (k,k) = 0$ in $A \times B$, then $n \mid k$ and $m \mid k$. If k is minimal positive integer, then $k = \operatorname{lcm}(n,m)$.

$\Rightarrow \boxed{\operatorname{char}(A \times B) = \operatorname{lcm}(n,m)}$

(c) Let $\gcd(n,m) = d > 1$. Then $\operatorname{lcm}(n,m) = \frac{nm}{d} < nm$. By (b), $\boxed{\operatorname{char}(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) = \operatorname{lcm}(n,m) = \frac{nm}{d}}$; $\boxed{\operatorname{char}(\mathbb{Z}/nm\mathbb{Z}) = nm} \neq \frac{nm}{d}$

$\Rightarrow$ the rings $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})$ and $(\mathbb{Z}/nm\mathbb{Z})$ are not isomorphic.

(d) The number of units in a ring $\mathbb{Z}/n\mathbb{Z}$ equals to the number of integers k, $1 \leq k \leq n$, coprime to n: $\gcd(k,n) = 1 \overset{\text{Bezout}}{\Leftrightarrow} \exists x, y \in \mathbb{Z}: kx + ny = 1 \Leftrightarrow k$ is invertible in $\mathbb{Z}/n\mathbb{Z}$

By definition, this number equals $\varphi(n)$.

If an element (a,b) is a unit in the ring $A \times B \Leftrightarrow \exists (a^{-1}, b^{-1}) \in A \times B$: $(a,b) \cdot (a^{-1}, b^{-1}) = (1,1) \Leftrightarrow a \in A$ is a unit and $b \in B$ is a unit

$\Rightarrow$ # units in $A \times B$ = (# units in A) $\cdot$ (# of units in B).

$\Rightarrow$ # units in $(\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}) = \varphi(9) \cdot \varphi(12) = (9-3)\cdot(4-2)\cdot(3-1) = \boxed{24}$

units in $(\mathbb{Z}/108\mathbb{Z}) = \varphi(108) = \varphi(3^3) \cdot \varphi(2^2) = (27-9)(4-2) = \boxed{36}$

(e) This is equivalent to showing $\underbrace{\varphi(n) \cdot \varphi(m)}_{\#\text{units in } \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}} \neq \underbrace{\varphi(nm)}_{\#\text{units in } \mathbb{Z}/nm\mathbb{Z}}$ if $\gcd(n,m) = d > 1$

Suppose p^t is a multiple of n, p^s is a multiple of m for a prime p, and $(p^t, \frac{n}{p^t}) = 1$, $(p^s, \frac{m}{p^s}) = 1$. Suppose $t \leq s$.

Then $\varphi(n)\varphi(m) = \varphi(p^t)\varphi(\frac{n}{p^t}) \cdot \varphi(p^s)\varphi(\frac{m}{p^s}) = (p^t - p^{t-1})(p^s - p^{s-1})\varphi(\frac{n}{p^t}) \cdot \varphi(\frac{m}{p^s})$

$\varphi(nm) = \varphi(p^{t+s}\frac{nm}{p^{t+s}}) = (p^{t+s} - p^{t+s-1})\varphi(\frac{nm}{p^{t+s}})$

We have: $(p^t - p^{t-1})(p^s - p^{s-1}) = p^{t+s} - 2p^{t+s-1} + p^{t+s-2} < p^{t+s} - p^{t+s-1}$ $\quad t, s \geq 1$

$\Leftrightarrow \quad p^{t+s-2} < p^{t+s-1}$

$\Rightarrow \frac{\varphi(n,m)}{\varphi(\frac{nm}{p^{t+s}})} > \frac{\varphi(n)\varphi(m)}{\varphi(\frac{n}{p^t})\varphi(\frac{m}{p^s})}$

Similarly, if $\gcd(\frac{n}{p^t}, \frac{m}{p^s}) > 1 \Rightarrow$ the multiple from the next prime in $\varphi(nm)$ > the multiple from that prime in $\varphi(n)\varphi(m)$.

Continuing by downward induction, arrive at coprime numbers $\Rightarrow \varphi(n,m) > \varphi(n)\varphi(m)$ if $\gcd(n,m) > 1$.

Second part, questions 9 to 12.

The following questions do not require any justification. Only your answer will be evaluated: +1 point for a correct answer, -1 for a wrong answer and 0 for no answer.

T 9. (True/False) The ideal $I = (6\mathbb{Z}) \cap (15\mathbb{Z}) \cap (10\mathbb{Z}) \subset \mathbb{Z}$ is equal to $(30\mathbb{Z})$.

T 10. (True/False) The polynomial $\overset{10}{3}X^7 + 12X^6 - 9X^4 - 24X^3 + 15X + \overset{3}{\cancel{10}}$ is irreducible in $\mathbb{Q}[X]$.

T 11. (True/False) There is a nontrivial group homomorphism between the cyclic groups $f : C_{15} \to C_{30}$.

F 12. (True/False) There is a nontrivial ring homomorphism $\phi : \mathbb{Z}/15\mathbb{Z} \to \mathbb{Z}/30\mathbb{Z}$.

[4 **points**]