MAS 4203 - EXAM 2 - Solution

1. Let $n \in \mathbb{Z}$, $n > 1$. Suppose $(n-1)! \equiv -1 \pmod{n}$.
Assume by way of contradiction that n is composite.
Then there is $a, b \in \mathbb{Z}$ such that

$$n = ab$$

and $1 < a, b < n$.
Then $2 \leq a \leq n-1$ and thus $a \mid (n-1)!$
Also $a \mid n$ and $n \mid (n-1)! + 1$ since
$(n-1)! \equiv -1 \pmod{n}$ & $n \mid (n-1)! + 1$.
Thus $a \mid (n-1)! + 1 - (n-1)! = 1$
which is a contradiction since $a > 1$.
Hence n must be prime.

2.
(i) An integer n is <u>pseudoprime</u> if n is composite and

$$2^n \equiv 2 \pmod{n}.$$

(ii) $561 = 3 \cdot 11 \cdot 17$ is composite.
To show $2^{561} \equiv 2 \pmod{561}$
it suffices to show $2^{561} \equiv 2 \pmod{m}$
for $m = 3, 11, 17$ since $3, 11, 17$ are pairwise rel. prime.
and this would imply
$m \mid (2^{561} - 2)$ for $m = 3, 11, 17$ &
$561 \mid (2^{561} - 2)$.

$2^2 = 4 \equiv 1 \pmod 3$.
$561 = 2 \cdot 280 + 1$,

$2^{561} = (2^2)^{280} 2^1 \equiv 1^{28} \cdot 2 \pmod 3$,
$2^{561} \equiv 2 \pmod 3$.

$2^{10} \equiv 1 \pmod{11}$ by Fermat's Little Theorem since
$p = 11$ is prime & $p \nmid 2$.

$2^{561} = (2^{10})^{56} \cdot 2^1 \equiv 1^{56} \cdot 2 \pmod{11}$,
$2^{561} \equiv 2 \pmod{11}$.

$2^{16} \equiv 1 \pmod{17}$ by Fermat's Little Theorem since
$p = 17$ is prime & $p \nmid 2$.

$561 = 35 \cdot 16 + 1$,

$2^{561} = (2^{16})^{35} \cdot 2^1 \equiv 1^{35} \cdot 2 \pmod{17}$,
$2^{561} \equiv 2 \pmod{17}$.

Hence $2^{561} \equiv 2 \pmod m$ for $m = 3, 11, 17$
as required & 561 is pseudoprime.

3.

(i) Euler's Theorem Let $a, m \in \mathbb{Z}$ with $m \geq 1$ and $(a, m) = 1$. Then

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

(ii) Let m, n be positive relatively prime integers. Then

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 + 0 \pmod{n},$$
$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 0 + 1 \pmod{m}$$

by Euler's Thm since $(m, n) = 1$ & $\varphi(m), \varphi(n) \geq 1$.

Hence

$$n \mid (m^{\varphi(n)} + n^{\varphi(m)} - 1), \quad m \mid (m^{\varphi(n)} + n^{\varphi(m)} - 1)$$

and

$$mn \mid (m^{\varphi(n)} + n^{\varphi(m)} - 1) \quad \text{since } (m, n) = 1,$$

& therefore

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn}.$$

4(i) An arithmetic function f is <u>multiplicative</u> if

$$f(mn) = f(m) f(n)$$

whenever m, n are positive relatively prime integers

(iii) Suppose m, n are positive relatively prime integers.

Note m, n can not both be even since then $(m, n) \geq 2$ which is a contradiction.

There are 3 cases.

Case 1 m and n is odd

Then mn is odd.

& $f(mn) = 1 = (+1)(+1) = f(m) f(n)$.

Case 2 m is odd & n is even.

Then mn is even. &

$f(mn) = -1 = 1 \cdot (-1) = f(m) f(n)$

Case 3 m is even & n is odd.

Then mn is even. &

$f(mn) = -1 = (-1) \cdot 1 = f(m) f(n)$

In all cases $f(mn) = f(m) f(n)$ & f is multiplicative.

5. $3000 = 2^3 \cdot 3 \cdot 5^3$

$30 = 2 \cdot 3 \cdot 5$

$175 = 5^2 \cdot 7$.

(i) $\phi(3000) = \phi(2^3)\,\phi(3)\,\phi(5^3)$

$= (2^3 - 2^2) \cdot 2 \cdot (5^3 - 5^2)$

$= 4 \cdot 2 \cdot 25 \cdot 4 = 800$

(ii) $\tau(3000) = 4 \cdot 2 \cdot 4 = 32$

(iii) $\sigma(30) = \sigma(2)\,\sigma(3)\,\sigma(5)$

$= 3 \cdot 4 \cdot 6 = 72$

(iv) $\mu(30) = \mu(2)\,\mu(3)\,\mu(5) = (-1)^3 = (-1)$.

(v) $F(n)$ is multiplicative by Thm 3.1 since both $\tau(n)$ & $(\tau(n))^2$ are multiplicative.

$F(5^2) = 1 + (\tau(5))^2 + (\tau(5^2))^2$

$= 1 + 4 + 9 = 14$

$F(7) = 1 + (\tau(7))^2 = 1 + 4 = 5$

$F(175) = F(25)\,F(7) = 14 \cdot 5 = 70$.

[31413] 6.

(i) $(\sigma(n))^2 = \sum_{d|n} g(d)$.

By Möbius Inversion

$$g(n) = \sum_{d|n} (\sigma(d))^2 \mu\left(\frac{n}{d}\right)$$

$$g(25) = \sum_{d|25} (\sigma(d))^2 \mu\left(\frac{25}{d}\right)$$

$$= \sigma(1)^2 \mu(25) + (\sigma(5))^2 \mu(5) + (\sigma(25))^2 \mu(1)$$

$$= 0 + (1+5)^2(-1) + (1+5+5^2)^2 \cdot 1.$$

$$= -36 + 31^2 = 925.$$

(ii) If $4 \mid n$ then $\mu(n) = 0$.
If $9 \mid (n+1)$ then $\mu(n+1) = 0$. } (*)

We want

$n \equiv 0 \pmod 4$ &
$n \equiv 8 \pmod 9$.

Let

$n = 36k + 8$ (where $k \in \mathbb{Z}^+$)

For such n satisfies (*) &

$\mu(n) + \mu(n+1) = 0 + 0 = 0$

for infinitely many n.

aii) Let $2^n - 1$ be composite.

Then $\sigma(2^n - 1) > 1 + (2^n - 1) = 2^n$

$$\sigma(2^{n-1}(2^n - 1)) = \sigma(2^{n-1})\,\sigma(2^n - 1)$$

(since σ is multipl. & $(2^{n-1}, 2^n - 1) = 1$)

$$= (2^n - 1)\,\sigma(2^n - 1)$$

$$> (2^n - 1) \cdot 2^n = 2 \cdot (2^{n-1}(2^n - 1))$$

Hence $2^{n-1}(2^n - 1)$ is abundant.