MAS 4203 Spring 2016 Final Exam Part I

1.(i) We say $a \mid b$ (a divides b) if

$$b = ac$$

for some integer c.

(ii) Proposition Let $a, b \in \mathbb{Z}$ with a and b not both zero. Then

$$(a,b) = \min\{am+bn : m,n \in \mathbb{Z} \text{ \& } am+bn > 0\}.$$

(iii)

Suppose $(a,b)=1$ & $a \mid bc$.

Since $(a,b)=1$, $ax+by=1$ for some $x,y \in \mathbb{Z}$ by (ii)

Since $a \mid bc$, $bc = ad$ for some $d \in \mathbb{Z}$.

Then
$$c(ax+by) = c \cdot 1,$$
$$acx + bcy = c,$$
$$acx + ady = c, \quad (\text{since } bc = ad),$$
$$a(cx+dy) = c,$$

and $a \mid c$ since c, x, d, y & $cx+dy \in \mathbb{Z}$.

(iv) Suppose p is prime & $p \mid ab$.

Since p is prime $(a,p) = 1$ or p.

Case 1 $(a,p)=1$. Then by (iii) $p \mid b$.

Case 2 $(a,b)=p$. Then $p \mid a$.

Therefore either $p \mid a$ or $p \mid b$.

2(i) an integer $p > 1$ is prime if its only positive divisors are 1 & p.

(ii) Suppose by way of contradiction that there is an integer $m > 1$ that has no prime divisor. By the Well-Ordering Principle there is a smallest such integer say m_0; i.e. m_0 is the smallest integer > 1 that has no prime divisor. m_0 is not prime since otherwise it would have a prime divisor namely itself. So m_0 is composite &

$$m_0 = ab$$

for some integers a, b with $1 < a, b < m_0$.
Since m_0 is the smallest positive integer > 1 that has no prime divisor a must have a prime divisor p since $1 < a < m_0$. But

$p \mid a$ & $a \mid m_0$ which implies $p \mid m_0$ and m_0 has a prime divisor which is a contradiction. Hence every integer > 1 must have at least one prime divisor.

(iii) Suppose by way of contradiction there are only finitely many primes $p_1 = 2, p_2, \ldots, p_r$. say.

Let $N = (p_1 p_2 \cdots p_r) + 1$.
Then clearly N is an integer > 1.
So by (ii) N must have a prime divisor p.

& $p = p_j$ for some $1 \le j \le r$.

But

$p \mid N$ & $p = p_j \mid (p_1 p_2 \cdots p_r)$ & so

$p \mid (N - p_1 p_2 \cdots p_r) = 1$ which is impossible since $p > 1$. & we have a contradiction. Therefore there must be infinitely many primes.]

3

(i) We say a is congruent to b modulo m (& write $a \equiv b \pmod m$) if $m \mid (a-b)$.

(ii) Suppose $a \equiv b \pmod m$ & $c \equiv d \pmod m$.
Then $m \mid (a-b)$ & $m \mid (c-d)$. Therefore
$m \mid c(a-b) + b(c-d) = ac - bd$,
ie
$$ac \equiv bd \pmod m.$$

(iii) An integer n is pseudoprime if it is composite and $2^n \equiv 2 \pmod n$.

(iv) Clearly $561 = (3)(11)(17)$ is composite
We show $2^{561} \equiv 2 \pmod m$ for $m = 3, 11$ & 17.
This is sufficient since $3, 11, 17$ are pairwise relatively prime.

$2^2 = 4 \equiv 1 \pmod 3$ &
$2^{561} = (2^2)^{280} 2^1 \equiv 1^{280} \cdot 2 = 2 \pmod 3$.

$2^{10} \equiv 1 \pmod{11}$ by Fermat's Little Theorem
since $11 \nmid 2$ & 11 is prime.
& $2^{561} = (2^{10})^{56} 2^1 \equiv 1^{56} \cdot 2 = 2 \pmod{11}$.

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

So
$$2^{561} = (2^{16})^{35+1} \quad (\text{since } 561 = 16 \cdot 35 + 1)$$
$$\equiv 1^{35} \cdot 2^1 \pmod{17}$$
$$\equiv 2 \pmod{17}.$$

Thus 561 is pseudoprime since we have shown $2^{561} \equiv 2 \pmod m$ for $m = 3, 11$ & 17.

4.

(i) Let p be a positive integer.
Suppose $2^p - 1$ is prime. Then $2^p - 1 > 1$ & $p > 1$.
Suppose by way of contradiction that p is composite
i.e. $p = ab$
for some $a, b \in \mathbb{Z}$ with $1 < a, b < p$.
We know $x^b - 1 = (x-1)(1 + x + \cdots + x^{b-1})$ for $x \in R$.
So
$$2^p - 1 = (2^a)^b - 1 = (2^a - 1)(1 + 2^a + \cdots + 2^{a(b-1)})$$
and $2^a - 1 \mid 2^p - 1$ since
$1 + 2^a + \cdots + 2^{a(b-1)} \in \mathbb{Z}$.

But $1 < a < p$ so $1 < 2^a - 1 < 2^p - 1$
which contradicts $2^p - 1$ being prime. Hence
p must be prime.

(ii) Let n be a positive integer and
suppose

$$2^n + 1$$

is prime. Then

$$n = 2^m \cdot b$$

for some integer $m \geq 0$ and some $b \in \mathbb{Z}$ odd, $b \geq 1$.
We show that $b = 1$.
Suppose by way of contradiction $b \geqslant 3$.

$$(x+1)(1 - x + x^2 - + \cdots + x^{b-1})$$
$$= 1 - x - + \cdots + x^{b-1}$$
$$+ x \mp x^2 + \cdots - x^{b-1} + x^b$$
$$= (1 + x^b).$$

So

$$2^n + 1 = \left(2^{2^m}\right)^b + 1 = (1 + 2^{2^m})(1 - 2^{2^m} + \cdots + (2^{2^m})^{(b-1)})$$

&

$$1 < 1 + 2^{2^m} \mid 2^n + 1$$

since $1 - 2^{2^m} + - \cdots + (2^{2^m})^{(b-1)} \in \mathbb{Z}$.
But this is

$$1 < 1 + 2^{2^m} < 1 + 2^{2^m \cdot b} = 1 + 2^n$$

which contradicts $1 + 2^n$ being prime.
Hence $b = 1$, $n = 2^m$ & n is a power of 2.

5

(i) An arithmetic function $f(n)$ is multiplicative if $f(mn) = f(m)f(n)$ whenever $(m,n)=1$.

(ii) Suppose m, n are positive integers & $(m,n)=1$.
Since $(m,n)=1$ m, n can not both be even. There are 3 cases:

Case 1 m even & n odd.
Then $f(m)=-1$, $f(n)=1$ and $f(mn)=1$ since mn is even.
$f(mn)=-1 = (-1)(1) = f(m)f(n)$.

Case 2 m odd & n even. See Case 1.

Case 3 Both m, n are odd.
Then $f(m)=f(n)=1$ & $f(mn)=1$ since mn is odd. So
$f(mn)=1=1\cdot 1=f(m)f(n)$.

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

(iii) Observe that $g(n) = \sum_{d|n} f(d)$.

g is multiplicative, since f is multiplicative.

by Thm 3.1