MAS 4203 - EXAM 2 - Spring 2017

1.

(i) $(3, 453) = 3$ since $3 \mid 453$.

$3 \nmid 347$ since $3 \nmid 3+4+7 = 14$.

So the congruence $3x \equiv 347 \pmod{453}$ has no solutions $x \in \mathbb{Z}$.

So Statement is FALSE.

(ii) Suppose $n \in \mathbb{Z}$, $n > 1$, $(n-1)! \equiv -1 \pmod{n}$.

Suppose by way of contradiction that n is composite.

Then $n = ab$

for some $1 < a, b < n$, $a, b \in \mathbb{Z}$.

Now $a \mid (n-1)! = 1 \cdot 2 \cdot \cdots \cdot (n-1)$

since $1 \leq a \leq n-1$. But

$n \mid (n-1)! + 1$ since $(n-1)! \equiv -1 \pmod{n}$.

But $a \mid n$ so $a \mid (n-1)! + 1$. This implies

$a \mid 1 = ((n-1)! + 1) - (n-1)!$ which

is a contradiction since $a > 1$.

Thus n is prime.

2.

(i) n is pseudoprime if n is composite & $2^n \equiv 2 \pmod{n}$.

(ii) Clearly $645 = (3)(5)(43)$ is composite.

$2^2 = 4 \equiv 1 \pmod{3}$.

$2^{645} = (2^2)^{322} 2^1 \equiv 1^{322} \cdot 2 \pmod{3}$

$\equiv 2 \pmod{3}$ &

$3 \mid (2^{645} - 2)$.

161
4
644

$2^4 = 16 \equiv 1 \pmod{5}$.

$2^{645} = (2^4)^{161} 2^1 \equiv 1^{161} \cdot 2 \pmod{5}$

$\equiv 2 \pmod{5}$ &

$5 \mid (2^{645} - 2)$.

By Fermat's Little Theorem

$2^{42} \equiv 1 \pmod{43}$

since 43 is prime & $43 \nmid 2$.

$645 = 15 \cdot 43 = 15(42+1)$

$2^{645} = (2^{42})^{15} 2^{15} \equiv 1^{15} \cdot 2^{15} \pmod{43}$

$\equiv 2^{15} \pmod{43}$.

$2^6 = 64 \equiv 21 \pmod{43}$, $2^7 = 42 \equiv -1 \pmod{43}$

So $2^{15} = (2^7)^2 \cdot 2 \equiv (-1)^2 \cdot 2 \pmod{43}$

$\equiv 2 \pmod{43}$

Hence $2^{645} \equiv 2 \pmod{43}$ & $43 \mid 2^{645} - 2$.

$645 \mid (2^{645} - 2)$ since 3, 5, 43 divide 645 & they are pairwise rel. prime. Hence $2^{645} \equiv 2 \pmod{645}$ & 645 is pseudoprime.

3.

(i) Let $m \mid n$, $m, n \in \mathbb{Z}^+$. Then $n = md$ for some $d \in \mathbb{Z}^+$.

$x^d - 1 = (x-1)(x^{d-1} + \cdots + x + 1)$.

Let $x = 2^m$. Then

$$2^n - 1 = (2^m)^d - 1 = (2^m - 1)(2^{m(d-1)} + \cdots + 2^m + 1) \text{ &}$$

$2^m - 1 \mid 2^n - 1$ since $(2^{m(d-1)} + \cdots + 1) \in \mathbb{Z}$.

(ii) Suppose p is prime & $2^p - 1$ is composite.

By the Cor. to Fermat's Little Theorem

$$2^p \equiv 2 \pmod{p}$$

since p is prime.

Also $p \mid 2^p - 2 = (2^p - 1) - 1 = n - 1$ where $n = 2^p - 1$.

By (i), $n = 2^p - 1 \mid 2^{n-1} - 1$ &

$2^{n-1} \equiv 1 \pmod{n}$ &

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

Thus $n = 2^p - 1$ is pseudoprime (since it is also composite).

4.

[2] (i) f is multiplicative if
$$f(mn) = f(m)f(n)$$
for all positive relatively prime integers m, n.

[4] (ii) Suppose f is multiplicative. Then
$$f(1) = f(1\cdot 1) = f(1)f(1)$$
since $(1,1) = 1$. Then
$$f(1)(f(1)-1) = (f(1))^2 - f(1) = 0 \text{ &}$$
$$f(1) = 0 \quad \text{or} \quad f(1) = 1.$$

[4] (iii) Let $n = 2^\alpha \cdot 5^\beta$ where $\alpha, \beta \geq 1$
$$\phi(n) = (2^\alpha - 2^{\alpha-1})(5^\beta - 5^{\beta-1})$$
$$= 2^{\alpha-1}\cdot 5^{\beta-1}(5-1)$$
$$= \frac{n\cdot 4}{2\cdot 5} = \frac{2n}{5}.$$

So there are infinitely many integers n such that
$$\phi(n) = \frac{2n}{5}.$$

5.

3 (i) $10! = 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2$

$= (2 \cdot 5) \cdot (3^2) \cdot (2^3) \cdot 7 \cdot (2 \cdot 3) \cdot 5 \cdot 2^2 \cdot 3 \cdot 2^1$

$= 2^8 \cdot 3^4 \cdot 5^2 \cdot 7.$

3 (ii) (a) $\tau(10!) = 9 \cdot 5 \cdot 3 \cdot 2 = 270$

(b) $\phi(10!) = 10! \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7}$

$= 10! \times \frac{8}{35}$

$= 2^{11} \cdot 3^4 \cdot 5 = 829440$

(c) $\mu(10!) = 0$ since $2^2 \mid 10!$

4 (iii) $2^5 = 32 \equiv 9 \pmod{23}$.

$2^{10} \equiv 81 \equiv 12 \pmod{23}$, since $81 - 12 = 69 = 3 \cdot 23$.

$2^{11} \equiv 24 \equiv 1 \pmod{23}$

$\tau(10^{1000}) = \tau(2^{1000})\,\tau(5^{1000})$ (since τ mult.)

$= (2^{1001} - 1)\,\tau(5^{1000})$.

$1001 = 91 \cdot 11$

$2^{1001} = (2^{11})^{91} \equiv 1^{91} \equiv 1 \pmod{23}$.

$\therefore 23 \mid 2^{1001} - 1$ &

$23 \mid \tau(10^{1000})$.

6.

[2] (i) Mobius Inversia Formula

$$f(n) = \sum_{d|n} g(d) \quad \text{for } n \geq 1$$

iff

$$g(n) = \sum_{d|n} f(d)\,\mu\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$$

[4] (ii) $\sigma(n) = \sum_{d|n} d.$

Let $f(n) = \sigma(n)$, $g(n) = n$. By Möbius Inv.

$$n = \sum_{d|n} \mu(d)\,\sigma\left(\frac{n}{d}\right).$$

[4] (iii) $\tau(n) = \sum_{d|n} 1.$

Let $f(n) = \tau(n)$, $g(n) = 1$. By Möbius Inversion,

$$1 = \sum_{d|n} \mu(d)\,\tau\left(\frac{n}{d}\right).$$

~~MAS 4203 Homework 2 - Spring 2014~~ (p7.)

~~Section 3.1~~

~~#4 (p.80)~~

Let $n \in \mathbb{Z}$ with $n > 0$. Define the arithmetic function ρ by $\rho(1) = 1$ and $\rho(n) = 2^m$ where m is the number of distinct prime numbers in the prime factoriztion of n.

(a) ρ is multiplicative ~~but not completely multiplicative.~~

Proof. Let $m, n \in \mathbb{Z}$, $m, n \geq 1$ and suppose $(m, n) = 1$. We will show that

$$\rho(mn) = \rho(m)\rho(n).$$

The result is clearly true if m or $n = 1$. We assume $m, n > 1$. Suppose there are r distinct primes in the prime factorization of n and s distinct primes in the prime factorization of m. Then since m and n are relatively prime there are $r + s$ primes in the factorization of mn. Hence

$$\rho(mn) = 2^{r+s} = 2^r 2^s = \rho(m)\rho(n).$$

~~Finally we show that ρ is not completely multiplicative. Now $\rho(2) = 2$ and $\rho(2^2) = 2$ so that $\rho(2 \cdot 2) \neq \rho(2)\rho(2)$.~~ □

(b) Let

$$n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$$

be the prime factorization of n. Then

$$f(n) := \sum_{d|n} \rho(d) = \prod_{i=1}^{m} (1 + 2a_i).$$

Proof. First let p be prime and suppose a is a positive integer. Then

$$\begin{aligned} f(p^a) &= \sum_{d|p^a} \rho(d) \\ &= \rho(1) + \rho(p) + \rho(p^2) + \cdots \rho(p^a) \\ &= 1 + 2 + 2 + \cdots 2 = 1 + 2a. \end{aligned}$$

Therefore

$$\begin{aligned} f(n) &= f(p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}) \\ &= f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_m^{a_m}) \\ &\qquad \text{(since } \rho \text{ and hence } f \text{ are multiplicative by Theorem 3.1} \\ &= (1 + 2a_1)(1 + 2a_2) \cdots (1 + 2a_m) \\ &= \prod_{i=1}^{m} (1 + 2a_i). \end{aligned}$$