Math 356—Test II

April 22, 2009

Your Name:

Solve exactly six of the following eight problems. If you solve more than six problems, you must indicate which ones are to be graded.

(1) When eggs in a basket are removed 3, 4, 5, 6 at a time, there are 2, 3, 4, 5 eggs left in the basket respectively. Find the smallest number of eggs that could have been in the basket.

(2) Show that $a^{12} - 1$ is divisible by 35 if $\gcd(a, 35) = 1$.

(3) (a) Find the remainder when 55! is divided by 53. (b) Find the remainder when 2(50!) is divided by 53.

(4) Show that when $n > 1$ is a composite number, $\sigma(n) \geq 1 + n + \sqrt{n}$.

(5) Let $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ be the prime factorization of the integer $n > 1$. Let $f(d)$ be a multiplicative function that is never zero. Show that

$$\sum_{d|n} \mu(d)/f(d) = (1 - 1/f(p_1))(1 - 1/f(p_2)) \dots (1 - 1/f(p_r)).$$

(6) (a) In how many zeros does 500! terminate? (b) For which values of n does $n!$ terminate in 24 zeros?

(7) Use Euler's theorem to find the last digit of 7^{1000}.

(8) For any positive integer n, show that $\sum_{d|n} \mu^2(d)/\phi(d) = n/\phi(n)$. (Hint: Use the prime factorization for n and the multiplicative property of both sides of the equation.)

1

Solutions to Test II – Number Theory

(1) $x \equiv 2 \mod 3$ (1)

$x \equiv 3 \mod 4$ (2)

$x \equiv 4 \mod 5$ (3)

$x \equiv 5 \mod 6$. (4). // 3pts

~~From~~ (1),

$$x = 2 + 3k. \quad \text{2pt}$$

Plug into (2):

$$2 + 3k \equiv 3 \mod 4.$$

$$3k \equiv 1 \mod 4.$$

$$(-1)k \equiv 1 \mod 4 \Rightarrow k \equiv -1 \equiv 3 \mod 4.$$

Hence $k = 3 + 4\ell$, and $x = 2 + 3(3 + 4\ell) = 11 + 12\ell$.

2pts

Plug into (3):

$$11 + 12\ell \equiv 4 \mod 5$$

$$12\ell \equiv -7 \mod 5 \equiv 3 \mod 5.$$

$$\Rightarrow 2\ell \equiv 3 \mod 5 \Rightarrow 6\ell \equiv 9 \mod 5$$

$\Rightarrow \ell \equiv 9 \mod 5$. Hence $\ell = 9 + 5m$

$$x = 11 + 12(9 + 5m) = 119 + 60m.$$

2pts

Plug into (4):

$$119 + 60m \equiv 5 \mod 6$$

$$\Rightarrow 60m \equiv -114 \equiv 0 \mod 6$$

Since the left hand side is always $\equiv 0 \mod 6$, this equation is satisfies by all m.

Hence the solution is $x = 119 + 60m$.

Take $m = -1$, we have $x = 59$. 2pts

②

(2) Since $\gcd(a, 35) = \gcd(a, 5 \cdot 7) = 1$,

$\gcd(a, 5) = \gcd(a, 7) = 1$. 3 pts

Thus by Fermat's Thm,

$a^4 \equiv 1 \mod 5$ & $a^6 \equiv 1 \mod 7$. 3 pts

Hence $a^{12} \equiv 1 \mod 5$ & $a^{12} \equiv 1 \mod 7$.

Since $5 \mid a^{12}-1$ & $7 \mid a^{12}-1$, and $\gcd(5, 7) = 1$,

We have $5 \cdot 7 \mid a^{12}-1$. $35 \mid a^{12}-1$. 4 pts

(3) (a) 4 pts $55! = 1 \cdots \underline{53} \cdot 54 \cdot 55$, $55! \equiv 0 \pmod{53}$. 4 pts

6 pts (b) By Wilson's Thm, $52! \equiv -1 \pmod{53}$. 2 pts

Hence $50!\, 51 \cdot 52 \equiv 50!\,(-2)(-1) \equiv 2\,(50!)$

$\equiv -1 \pmod{53}$. 2 pt

Therefore $2\,(50!) \equiv -1 \pmod{53} \equiv 52 \pmod{53}$ 2 pts

(4) Let $n > 1$ be a composite number. Then

$n = a \cdot b$, $a, b \geq 2$. At least one of a, b

must be $\geq \sqrt{n}$, otherwise, if $a < \sqrt{n}$ & $b < \sqrt{n}$,

then $a \cdot b < n$, contradicting $n = a \cdot b$. Therefore,

n has at least factors 1, n, and a or b

(whichever $\geq \sqrt{n}$). Thus $\sigma(n) \geq 1 + n + \sqrt{n}$.

③

(5) First, since $\mu(d)$ & $f(d)$ are multiplicative and $f(d) \neq 0$, $\frac{\mu(d)}{f(d)}$ is also multiplicative, for if $\gcd(m,n)=1$,

$$\frac{\mu(m \cdot n)}{f(m \cdot n)} = \frac{\mu(m)\,\mu(n)}{f(m)\,f(n)} = \frac{\mu(m)}{f(m)} \cdot \frac{\mu(n)}{f(n)},$$

Hence

$$F(n) = \sum_{d|n} \frac{\mu(d)}{f(d)} \text{ is multiplicative.}$$

Now, when $n = p^k$, p - prime, $k \geq 1$, then

$$F(p^k) = \frac{\overbrace{\mu(1)}^{=1}}{f(1)} + \frac{\overbrace{\mu(p)}^{=-1}}{f(p)} + \frac{\overbrace{\mu(p^2)}^{=0}}{f(p^2)} + \cdots + \frac{\overbrace{\mu(p^k)}^{=0}}{f(p^k)}$$

$$= \frac{1}{f(1)} - \frac{1}{f(p)}.$$

Since $f(p) = f(p \cdot 1) = f(p) \cdot f(1)$ & $f(p) \neq 0$

$\Rightarrow f(1) = 1$. Hence $F(p^k) = 1 - \frac{1}{f(p)}$.

When $n = p_1^{k_1} \cdots p_r^{k_r}$, by the multiplicative of F,

$$F(n) = F(p_1^{k_1} \cdots p_r^{k_r}) = F(p_1^{k_1}) \cdots F(p_r^{k_r})$$

$$= \left(1 - \frac{1}{f(p_1)}\right) \cdots \left(1 - \frac{1}{f(p_r)}\right), \text{ as desired.}$$

(6) (a) Since

$5\cancel{p}^{y}$ $\left[\frac{500}{5}\right] + \left[\frac{500}{5^2}\right] + \left[\frac{500}{5^3}\right] = 100 + 20 + 4$
$= 124.$

The # of zeros is 124.

④

(b) $\left[\frac{n}{5}\right] + \left[\frac{n}{25}\right] + \cdots = 24$

5 pts

$\Rightarrow \quad \frac{n}{5} + \frac{n}{25} \approx 24. \qquad \frac{6}{25} n \approx 24$

$n \approx 100.$

Now check:

$$\left[\frac{99}{5}\right] + \left[\frac{99}{25}\right] = 19 + 3 = 22$$

$$\left[\frac{100}{5}\right] + \left[\frac{100}{25}\right] = 20 + 4 = 24$$

$$\left[\frac{101}{5}\right] + \left[\frac{101}{25}\right] = 20 + 4 = 24$$

$$\cdots$$

$$\left[\frac{104}{5}\right] + \left[\frac{104}{25}\right] = 20 + 4 = 24$$

$$\left[\frac{105}{5}\right] + \left[\frac{105}{25}\right] = 21 + 4 = 25.$$

Therefore, the values of n are: 100, 101, 102, 103, 104.

(7) Since $\gcd(7, 10) = 1$, and $\phi(10) = \phi(2)\phi(5) = 1 \cdot 4 = 4$,

We have by Euler's Thm,

$$7^4 \equiv 1 \mod 10.$$

Hence $(7^4)^{250} = 7^{1000} \equiv 1 \mod 10.$

The last digit is 1.

⑤

(8) As in Problem #5,

$\frac{\mu^2(d)}{\phi(d)}$ is multiplicative and hence so is

$$F(n) = \sum_{n|d} \frac{\mu^2(d)}{\phi(d)}.$$

When $n = p^k$, p - prime, $k \geq 1$,

$$F(p^k) = \frac{\mu^2(1)}{\phi(1)} + \frac{\mu^2(p)}{\phi(p)} + \frac{\overbrace{\mu^2(p^2)}^{=0}}{\phi(p^2)} + \cdots + \frac{\overbrace{\mu^2(p^k)}^{=0}}{\phi(p^k)}$$

$$= \frac{1}{1} + \frac{1}{p-1} = 1 + \frac{1}{p-1} = \frac{p}{p-1}.$$

For $n=1$, $F(1) = \frac{\mu^2(1)}{\phi(1)} = 1 = \frac{1}{\phi(1)}$, the identity holds.

For $n > 1$, let $n = p_1^{k_1} \cdots p_r^{k_r}$ be the prime factorization. Then

$$F(n) = F(p_1^{k_1}) \cdots F(p_r^{k_r}) = \frac{p_1}{p_1 - 1} \cdots \cdot \frac{p_r}{p_r - 1}.$$

On the other hand,

$$\frac{n}{\phi(n)} = \frac{p_1^{k_1} \cdots p_r^{k_r}}{(p_1^{k_1} - p_1^{k_1-1}) \cdots (p_r^{k_r} - p_r^{k_r-1})} = \frac{p_1 \cdots p_r}{(p_1-1)\cdots(p_r-1)}$$

$$= F(n).$$

Therefore $F(n) = \frac{n}{\phi(n)}$ as desired.