

## PRACTICE MIDTERM II SOLUTIONS

1. For which  $n$  does  $\phi(n)|n$  ?

**Solution:** Write  $n = 2^a p_1^{b_1} \cdots p_k^{b_k}$  where  $p_i$  are distinct odd primes. We have

$$\phi(n) = 2^{a-1} p_1^{b_1-1} (p_1 - 1) \cdots p_k^{b_k-1} (p_k - 1)$$

so that

$$\frac{n}{\phi(n)} = \frac{2p_1 \cdots p_k}{(p_1 - 1) \cdots (p_k - 1)}$$

Now, the denominator is divisible by  $2^k$  and the numerator by 2, so that  $k \leq 1$ . We have therefore reduced to the case  $n = 2^a p^b$  where  $p$  is an odd prime. Now,

$$\frac{n}{\phi(n)} = \frac{2p}{p-1}$$

and  $p-1 = 2s$  for some integer  $s < p-1$ . Thus  $\frac{n}{\phi(n)} = \frac{p}{s}$ , and if  $s > 1$  this is not an integer. Therefore  $p-1 = 2$ , and  $p = 3$ . Thus  $n = 1$  or  $n = 2^a 3^b$ ,  $a \geq 1, b \geq 0$ .

2. Suppose that  $f$  is a multiplicative function. Show that

$$\sum_{d|n} \mu(d) f(d) = (1 - f(p_1))(1 - f(p_2)) \cdots (1 - f(p_k))$$

where  $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$  is the prime power factorization of  $n$ .

**Solution:** Since  $\mu$  and  $f$  are both multiplicative, so is  $\mu \cdot f$ . Furthermore, if  $h$  is a multiplicative function, so is

$$g(n) = \sum_{d|n} h(d).$$

Therefore the function

$$g(n) = \sum_{d|n} \mu(d) \cdot f(d)$$

is multiplicative.  $g(p^a) = f(1) - f(p) = 1 - f(p)$  for a prime  $p$  since  $\mu(p^k) = 0$  when  $k \geq 2$ . By multiplicativity we have

$$g(p_1^{a_1} \cdots p_k^{a_k}) = (1 - f(p_1)) \cdots (1 - f(p_k))$$

5. Let  $m = a^n - 1$  where  $a$  and  $n$  are positive integers. Show that  $n|\phi(m)$ .

**Solution:** (for this problem to make sense,  $a > 1$ ) We have  $a^n \equiv 1 \pmod{m}$ , so that  $\text{ord}_m(a)|n$ . In fact  $\text{ord}_m(a) = n$ , since  $a^k < m$  for  $k < n$ , making  $a^k \equiv 1 \pmod{m}$  impossible. Now  $\text{ord}_m(a)|\phi(m)$  implies  $n|\phi(m)$ .

6. What are the primitive roots  $\text{mod } 7^3$  ?

**Solution:** Given an odd prime  $p$ , we know that there are  $\phi(\phi(p^2)) = (p-1)\phi(p-1)$  primitive roots  $\pmod{p^2}$ . By Prop. 4.6, if  $g$  is a primitive root  $\pmod{p^2}$ , then any lift  $h \pmod{p^3}$  such that  $g \equiv h \pmod{p^2}$  is a primitive root  $\pmod{p^3}$ . For each  $g \pmod{p^2}$ , there are  $p$  lifts of  $g$  to residues  $\pmod{p^3}$ , for a total of  $p(p-1)\phi(p-1)$  residues  $\pmod{p^3}$  that are primitive roots  $\pmod{p^3}$ . Since  $\phi(\phi(p^3)) = p(p-1)\phi(p-1)$ , these are all of the primitive roots  $\pmod{p^3}$ . To answer our question, it suffices to find a single primitive root  $\text{mod } 7^2$ , say  $a$ . The other primitive roots  $\pmod{7^2}$  are  $a^s$  where  $\gcd(s, \phi(7^2)) = 1$ . The primitive roots  $\pmod{7^3}$  are  $a^s + 7k$ , where  $\gcd(s, \phi(7^2)) = 1, 0 \leq k < 7$ . For instance,  $a = 3$  works.

7. Show that if  $b$  is a positive integer not divisible by the prime  $p$ , then

$$\left(\frac{b}{p}\right) + \left(\frac{2b}{p}\right) + \left(\frac{3b}{p}\right) + \cdots + \left(\frac{(p-1)b}{p}\right) = 0$$

**Solution:**

$$\begin{aligned} & \left(\frac{b}{p}\right) + \left(\frac{2b}{p}\right) + \left(\frac{3b}{p}\right) + \cdots + \left(\frac{(p-1)b}{p}\right) \\ &= \left(\frac{b}{p}\right) \left[ \left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \left(\frac{3}{p}\right) + \cdots + \left(\frac{p-1}{p}\right) \right] \end{aligned}$$

Now,  $\pmod{p}$  there are  $(p-1)/2$  quadratic residues and the same number of quadratic non-residues. Thus, in the summation in brackets, we get  $(p-1)/2$  terms that are  $+1$  and the same number that are  $-1$ , which implies that

$$\left[ \left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \left(\frac{3}{p}\right) + \cdots + \left(\frac{p-1}{p}\right) \right] = 0$$