Math 115B: Solutions to Practice Problems for Midterm

1. True or False: a) If $\left(\frac{a}{p}\right) \cdot \left(\frac{a}{q}\right) = 1$, then a is a quadratic residue modulo pq. **False.**

   b) If $F(n) = \sum_{d|n} f(d)$ where F, f are arithmetic functions and F is multiplicative, then f is multiplicative. **True.**

   c) $\sigma(n) \geq \tau(n)$ for all $n \in \mathbb{N}$. **True.**

   d) 70 is a quadratic residue modulo 71. **False.**

   e) There are 35 quadratic non-residues modulo 71. **True.**

2. Let
$$f(n) = \frac{\phi(n)}{\sigma(n)}$$

   (a) Show that f is a multiplicative function.

   SOLUTION: We have shown in class that ϕ and σ are multiplicative. Hence we have that if $(m, n) = 1$,
$$f(nm) = \frac{\phi(nm)}{\sigma(nm)} = \frac{\phi(n)}{\sigma(n)} \cdot \frac{\phi(m)}{\sigma(m)} = f(n)f(m),$$
   so f is multiplicative.

   (b) Show that $f(n) < 1$ for all $n > 1$.

   SOLUTION: If $n > 1$, then $\phi(n) < n$, while $\sigma(n) \geq n+1$ (since n and 1 are always distinct divisors of n), so we have $\phi(n) < \sigma(n)$ and hence $f(n) < 1$ if $n > 1$.

3. Find $\tau(720)$, $\phi(720)$, $\sigma(720)$.

   SOLUTION: Note that $720 = 2^4 \cdot 3^2 \cdot 5$. Hence by multiplicativity of these three arithmetic functions
$$\tau(720) = \tau(2^4)\tau(3^2)\tau(5) = (4+1)(2+1)(1+1) = 30$$
$$\phi(720) = \phi(2^4)\phi(3^2)\phi(5) = 2^3(2-1)3(3-1)4$$
   No need to simplify the answer!
$$\sigma(720) = \sigma(2^4)\sigma(3^2)\sigma(5) = \frac{2^5-1}{2-1}\frac{3^3-1}{3-1}\frac{5^2-1}{5-1}$$

No need to simplify the answer!

4. Find a number n with $\tau(n) = 25$.

   SOLUTION: For example, if $n = p^{24}$ where p is a prime then $\tau(n) = 24 + 1 = 25$. So e.g. 2^{24} works.

5. Show that if p is an odd prime then

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$$

   where $\left(\frac{a}{p}\right)$ denotes the Legendre symbol.

   SOLUTION: We have shown in class that for an odd prime p exactly half of the numbers between 1 and $p-1$ are quadratic residues modulo p. Hence the above sum is the sum of $\frac{p-1}{2}$ 1's and $\frac{p-1}{2}$ -1's and hence the sum is 0.

6. Suppose $n = 6 \cdot p$ where $p \geq 5$ is a prime. Show that

$$\sigma(n) > 2n$$

   SOLUTION:

$$\sigma(6p) = \sigma(6)\sigma(p) = 2 \cdot 6\sigma(p) > 2 \cdot 6p = 2n$$

7. Use Euler's criterion to calculate the Legendre symbol

$$\left(\frac{3}{17}\right)$$

   SOLUTION:

   We need to calculate $3^{(17-1)/2}$ i.e. 3^8 modulo 17. Note that

$$3^3 = 27 \equiv 10 \mod 17$$

   Hence

$$3^8 \equiv 10 \cdot 10 \cdot 9 \equiv 15 \cdot 9 \equiv -2 \cdot 9 \equiv -1 \mod 17$$

   Hence by Euler's criterion

$$\left(\frac{3}{17}\right) = -1$$

8. Show that n is perfect if and only if

$$\sum_{d|n, d\geq 1} \frac{1}{d} = 2$$

SOLUTION: n is perfect if and only if

$$\sigma(n) = 2n$$

i.e.

$$\sum_{d|n} \frac{d}{n} = 2$$

This can be written as

$$2 = \sum_{d|n} \frac{1}{n/d} =^{!} \sum_{d|n} \frac{1}{d}$$

as desired.

9. Show that if n is perfect then there is no integer $s \geq 2$ such that sn is also perfect.

SOLUTION: If n is perfect then

$$\sum_{d|n} \frac{1}{d} = 2$$

Now every divisor of n is a divisor of sn and if $s > 1$ then sn will have some additional divisors. Hence

$$\sum_{d|sn} \frac{1}{d} = \sum_{d|n} \frac{1}{d} + \text{something positive} = 2 + \text{something positive} > 2$$

and hence sn can't be perfect.

10. Let Ω be the following arithmetic function: $\Omega(n)$ is the number of prime factors of n, including repetitions. So e.g. $\Omega(1) = 0$, $\Omega(3 \cdot 5) = 2$ and $\Omega(2^2 3) = 3$. Suppose f is an arithmetic function such that

$$\Omega(n) = \sum_{d|n, d\geq 1} f(d).$$

Find explicitly the value

$$f(15)$$

SOLUTION: By Mobius inversion one has

$$f = \sum_{d|n, d\geq 1} \Omega(d) * \mu(n/d)$$

In particular,

$$f(15) = \sum_{d|15} \Omega(d)\mu(15/d)$$

This equals

$$\Omega(1) - \Omega(3) - \Omega(5) + \Omega(15) = 0 - 1 - 1 + 2 = 0$$

Hence

$$f(15) = 0$$

11. Determine the set of primes modulo which 7 is a quadratic residue.

    SOLUTION: First of all, 7 is certainly a quadratic residue modulo 2. Now, given an odd prime p, we have that

    $$\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right)$$

    if $p \equiv 1 \pmod 4$, and

    $$\left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right)$$

    if $p \equiv 3 \pmod 4$. Noting that p is a quadratic residue mod 7 if $p \equiv 1, 2, 4 \pmod 7$, and a quadratic non-residue if $p \equiv 3, 5, 6 \pmod 7$, we get that 7 is a quadratic residue mod p if $p \equiv 1 \pmod 4$ and $p \equiv 1, 2,$ or $4 \pmod 7$, or $p \equiv 3 \pmod 4$ and $p \equiv 3, 5,$ or $6 \pmod 7$. Using the Chinese remainder theorem, we get that 7 is a quadratic residue mod p iff p is 2 or $p \equiv 1, 9, 25, 3, 19,$ or $27 \pmod{28}$.

12. Find the collection of all integers that are of the form $\text{ord}_{151}(a)$ where a ranges through the integers co-prime to 151.

13. (a) Find all primitive roots modulo 13.

    SOLUTION: There are $\phi(\phi(13)) = \phi(12) = 4$ primitive roots $\pmod 13$. We check and find that 2 is a primitive root, meaning its order is 12 mod 13. Hence, if i is relatively prime to 12, 2^i is also of order 12. Thus 2^5, 2^7, and 2^11 are also primitive roots, and these are $6, 11, 7 \pmod 13$. Thus we have found all 4 primitive roots, and they are $2, 6, 11, 7$.

    (b) How many primitive roots are there modulo 171?

    SOLUTION: 171 is $9 \cdot 19$, and by the primitive root theorem there are no primitive roots modulo a number of this form (since it is not a power of a prime, or twice the power of a prime).

(c) How many primitive roots are there modulo 173?

SOLUTION: 173 is prime, so there are $\phi(\phi(173)) = \phi(172) = \phi(4 \cdot 43) = 2 \cdot 42 = 84$ primitive roots $\pmod 173$.

14. How many primitive roots are there modulo 12^{100}?

SOLUTION: None: by the Primitive Root Theorem, only modulo numbers of the form 1, 2, 4, p^m, and $2 \cdot p^m$ where p is an odd prime and $m \geq 1$ is an integer can one have a primitive root.

15. Find the order of 12 modulo 25.

SOLUTION: This order must divide $\phi(25) = 20$, so it can only be $2, 4, 5, 10$, or 20. Taking these powers of 12 modulo 25, we get that 12 is in fact a primitive root $\pmod 25$, and so its order is 20.