Homework 7
(Quadratic reciprosity, arithmetic/multiplicative functions,
Mobius inversion, the Dirichlet product.)
Due Wednesday, November 13 at 11:30am in class.

Note: Be sure to justify your answers. No credit will be given for answers without work/justification. In addition, all written homework assignments should be neat and well-organized; **this assignment has only one part and can be submitted as a single packet**.

(1) Use the Law of Quadratic Reciprocity to determine if 73 is a quadratic residue mod 191. We have that 73 and 191 are both prime and only one is congruent to 3 mod 4. So

$$\begin{aligned}\left(\frac{73}{191}\right) &= \left(\frac{191}{73}\right) = \left(\frac{45}{73}\right) = \left(\frac{3}{73}\right)^2\left(\frac{5}{73}\right) \\ &= \left(\frac{5}{73}\right) = \left(\frac{73}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right).\end{aligned}$$

Since $Q_3 = \{[1]\}$, we have that $\left(\frac{73}{191}\right) = \left(\frac{2}{3}\right) = -1$. Thus 73 is not a quadratic residue mod 191.

(2) Use the Law of Quadratic Reciprocity to show that, for p prime,

$$[7] \in Q_p \text{ if and only if } p = 2 \text{ or } p \equiv \pm 1, \pm 3, \pm 9 \pmod{28}.$$

Proof. We have that

$$\begin{aligned}[7] \in Q_p \text{ iff } &\left(\frac{7}{p}\right) = 1 \\ \text{iff } &\left(p \equiv 1 \pmod 4 \text{ AND } \left(\frac{p}{7}\right) = 1\right) \\ &\quad \text{OR} \\ &\left(p \equiv 3 \pmod 4 \text{ AND } -\left(\frac{p}{7}\right) = 1\right).\end{aligned}$$

We compute that, for p an *odd* prime,

$$\left(\frac{p}{7}\right) = \begin{cases} 0 & \text{if } p \equiv 0 \pmod 7 \\ 1 & \text{if } p \equiv 1, 2, 4 \pmod 7 \\ -1 & \text{if } p \equiv 3, 5, 6 \pmod 7 \end{cases}$$

We have that $p \equiv 1 \pmod 4$ and $p \equiv 1, 2, 4 \pmod 7$ if and only if $p \equiv 1, 9, 25 \pmod{28}$. (To see this, apply the Chinese Remainder Theorem in each case.) Similarly, we have that $p \equiv 3 \pmod 4$ and $p \equiv 3, 5, 6 \pmod 7$ if and only if $p \equiv 3, 19, 27 \pmod{28}$. □

(3) An arithmetic function f is called *completely multiplicative* if $f(ab) = f(a)f(b)$ for all $a, b \in \mathbb{N}$. For example, for a fixed prime p, the Legendre symbol $\left(\frac{a}{p}\right)$ is a completely multiplicative function.

(a) Determine if $\tau(n)$ is completely multiplicative. If it is, prove it. If not, find values of a and b for which $\tau(ab) \neq \tau(a)\tau(b)$.
$\tau(n)$ is not completely multiplicative. Let $a = 2$ and $b = 6$. Then $\tau(2) = 2$ and $\tau(6) = 4$, but $\tau(12) = 6 \neq 8$.

(b) Fix $m \in \mathbb{N}$. Let $f(n) = \gcd(m, n)$. Show that f is a multiplicative function. Is it completely multiplicative?

Proof. Fix $m \in \mathbb{N}$. Let $f(n) = \gcd(m, n)$. Let $n_1, n_2 \in \mathbb{N}$ such that $\gcd(n_1, n_2) = 1$. We want to show that

$$\gcd(m, n_1 n_2) = \gcd(m, n_1)\gcd(m, n_2).$$

Let's show that each side divides the other. Let

$$d = \gcd(m, n_1 n_2), d_1 = \gcd(m, n_1), \text{ and } d_2 = \gcd(m, n_2).$$

Recall the following theorem:

$$c \mid a \text{ and } c \mid b \text{ if and only if } c \mid \gcd(a, b)$$

Show that $d \mid d_1 d_2$ **:** By Bezout's identity, there are $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ such that

$$d_1 = a_1 m + b_1 n_1 \text{ and } d_2 = a_2 m + b_2 n_2.$$

Therefore,

$$d_1 d_2 = (a_1 m + b_1 n_1)(a_2 m + b_2 n_2) = a_1 a_2 m^2 + a_1 b_2 m n_2 + a_2 b_1 m n_1 + b_1 b_2 n_1 n_2.$$

We know that $d \mid m$ and $d \mid (n_1 n_2)$ by definition of the gcd. Thus d divides each term in $d_1 d_2$ above. So $d \mid d_1 d_2$, as desired.
Show that $d_1 d_2 \mid d$ **:** Since $d_1 \mid n_1$ and $d_2 \mid n_2$, we know that $d_1 d_2 \mid n_1 n_2$. Recall the following theorem:

$$c \mid a \text{ and } c \mid b \text{ if and only if } c \mid \gcd(a, b).$$

Thus we only need to show $d_1 d_2 \mid m$ and we'll be done. Since $d_1 \mid m$ and $d_2 \mid m$, if $\gcd(d_1, d_2) = 1$, then $d_1 d_2 \mid m$. (This follows from Corollary 1.11(a).) So say that $\gcd(d_1, d_2) = a$. Then $a \mid d_1$ and $d_1 \mid n_1$, so $a \mid n_1$ by transitivity. Similarly, $a \mid n_2$. Since $\gcd(n_1, n_2) = 1$, this implies that $a = 1$.
Thus $d \mid d_1 d_2$ and $d_1 d_2 \mid d$ so $d = d_1 d_2$, as desired. □

This function is not usually completely multiplictative. For example

$$\gcd(m, 2)\gcd(m, 2) \neq \gcd(m, 4)$$

for any even m not divisible by 4. However, if $m = 1$, then $\gcd(1, n_1)\gcd(1, n_2) = 1\dot{1} = 1 = \gcd(1, n_1 n_2)$.

(4) Use the inductive definition of the Mobius function $\mu(n)$ to compute $\mu(150)$. You may not use the theorem giving the closed formula (Theorem 8.8), but you may use that $\mu(p) = -1$ for a prime p. We have that

$$0 = \sum_{d|150} \mu(d) = \mu(1) + \mu(2) + \mu(3) + \mu(5) + \mu(6) + \mu(10) + \mu(15) + \mu(25) + \mu(30) + \mu(50) + \mu(75) + \mu(150).$$

We have that $\mu(1) = 1$ and $\mu(2) = \mu(3) = \mu(5) = -1$. Computing:

- $0 = \sum_{d|6} \mu(d) = \mu(1) + \mu(2) + \mu(3) + \mu(6) = 1 - 1 - 1 + \mu(6)$, so $\mu(6) = 1$.
- $0 = \sum_{d|10} \mu(d) = \mu(1) + \mu(2) + \mu(5) + \mu(10) = 1 - 1 - 1 + \mu(10)$, so $\mu(10) = 1$.

- $0 = \sum_{d|15} \mu(d) = \mu(1) + \mu(3) + \mu(5) + \mu(15) = 1 - 1 - 1 + \mu(15)$, so $\mu(15) = 1$.
- $0 = \sum_{d|25} \mu(d) = \mu(1) + \mu(5) + \mu(25) = 1 - 1 + \mu(25)$, so $\mu(25) = 0$.
- $0 = \sum_{d|30} \mu(d) = \mu(1) + \mu(2) + \mu(3) + \mu(5) + \mu(6) + \mu(10) + \mu(15) + \mu(30)$
  . $= 1 - 1 - 1 - 1 + 1 + 1 + 1 + \mu(30)$, so $\mu(30) = -1$.
- $0 = \sum_{d|50} \mu(d) = \mu(1) + \mu(2) + \mu(5) + \mu(10) + \mu(25) + \mu(50)$
  . $= 1 - 1 - 1 + 1 + 0 + \mu(50)$, so $\mu(50) = 0$.
- $0 = \sum_{d|75} \mu(d) = \mu(1) + \mu(3) + \mu(5) + \mu(15) + \mu(25) + \mu(75)$
  . $= 1 - 1 - 1 + 1 + 0 + \mu(75)$, so $\mu(75) = 0$.

Returning to our original equation, we have that

$$0 = 1 - 1 - 1 - 1 + 1 + 1 + 1 + 0 - 1 + 0 + 0 + \mu(150).$$

So $\mu(150) = 0$.

(5) (a) For each positive integer n, show that

$$\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0.$$

Proof. Note that for any sequence of 4 consecutive integers, at least one of the four is divisible by 4. For that integer, $\mu = 0$ by Theorem 8.8. Thus the product is 0. □

(b) For any integer $n \geq 3$, show that

$$\sum_{k=1}^{n} \mu(k!) = 1.$$

Proof. Note that for $k \geq 4$, by part (a), $\mu(k!) = 0$. So

$$\sum_{k=1}^{n} \mu(k!) = \mu(1!) + \mu(2!) + \mu(3!) = \mu(1) + \mu(2) + \mu(6) = 1 - 1 + 1 = 1.$$

□