18.781
PROBLEM SET 6

JOHN WANG

1. Problem 1

Problem 1.1. *Show that* $\prod_{d|n} d = n^{d(n)/2}$.

Solution We note that if d is a divisor of n, then $\frac{n}{d}$ must also be a divisor of n which is distinct from d, since clearly $d|n$ by definition. The divisor must be distinct unless n is a square, and $d^2 = n$, but we shall still count those as two distinct divisors.

Since each divisor d must also have a pair $\frac{n}{d}$, and we know that the product of the pair is n, we can match up all of the divisors of n in the following way, letting d_i be the first divisor in the pair:

$$\prod_{d|n} d = \prod_{i=1}^{d(n)/2} d_i \frac{n}{d_i} \tag{1.1}$$

$$= \prod_{i=1}^{d(n)/2} n \tag{1.2}$$

$$= n^{d(n)/2} \tag{1.3}$$

□

2. Problem 2

Problem 2.1. *If k is a positive integer, show that $\sigma_k(n)$ is odd if and only if n is a square or twice a square.*

Solution First, we note that $\sigma_k(n)$ is a multiplicative function so that $\sigma_k(ab) = \sigma_k(a)\sigma_k(b)$ as shown in class. Also, we know that $\sigma_k(p^e) = 1 + p^k + p^{2k} + \ldots + p^{ek}$ because the only divisors of p^e are $1, p, p^2, \ldots, p^e$. Summing up the kth powers gives the expression. Therefore, we can decompose $\sigma_k(n)$ for any arbitrary integer n using the prime factorization theorem, where $n = 2^{e_0} p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$:

$$\sigma_k(n) = \sigma_k(2^{e_0})\sigma_k(p_1^{e_1})\sigma_k(p_2^{e_2})\ldots\sigma_k(p_r^{e_r}) \tag{2.1}$$

$$= (1 + 2 + 2^2 + \ldots + 2^{e_0})(1 + p_1^k + p_1^{2k} + \ldots + p_1^{e_1 k}) \ldots \left(1 + p_r^k + p_r^{2k} + \ldots + p_r^{e_r k}\right) \tag{2.2}$$

Now, we see that $(1 + 2 + 2^2 + \ldots 2^{e_0})$ must always be odd, because 2^i for $i \geq 1$ is always even, so that $\sum_{i=1}^{e_0} 2^i$ is also even. This means that $1 + \sum_{i=1}^{e_0} 2^i = 1 + 2 + 2^2 + \ldots 2^{e_0}$ must be odd. Now, we invoke the following lemma:

Lemma 2.3. *Let p be an odd prime. The sum $1 + p^k + p^{2k} + \ldots + p^{ek}$ is odd if and only if e is even.*

Proof. We know that any odd integer multiplied by another odd integer results in an odd integer. Thus, p^k must be odd because p is an odd prime. This means that each term in the sequence $\{p^k, p^{2k}, \ldots, p^{ek}\}$ must be odd because they are just p^k multiplied by more odd numbers.

Moreover, we know that a sum of odd numbers is odd if and only if there are an odd number of them. This implies that there must be an odd number of terms in $1 + p^k + p^{2k} + \ldots + p^{ek}$ in order for it to be odd. This occurs if and only if e is even. □

Now, if all of the e_i are even, we can rewrite $e_1, e_2, \ldots, e_r$ in the form $k_i = e_i/2$, and set:

$$k_0 = \begin{cases} \frac{e_0}{2} & \text{if } e_0 \text{ is even} \\ \frac{e_0 - 1}{2} & \text{if } e_0 \text{ is odd} \end{cases} \tag{2.4}$$

Notice that we can do this if and only if n is a square because $n = (2^{k_0} p_1^{k_1} \ldots p_r^{e_k})^2$ if e_0 is even or $n = 2(2^{k_0} p_1^{k_1} \ldots p_r^{e_k})^2$ if e_0 is odd. However, if all e_i are even the, by the lemma shown above, each term $\sigma_k(p_i^{e_i})$ must be odd, so the product of all these terms must also be odd. Notice that this happens if and only if n is a square in one of the above two forms. □

3. Problem 3

Problem 3.1. *Prove that if $(a,b)>1$ then $\sigma_k(ab)<\sigma_k(a)\sigma_k(b)$ and $d(ab)<d(a)d(b)$.*

Solution First, we note that $\sigma_k(n)=\sum_{d|n} d^k$ by definition. However, we can decompose n into is prime factors $n=p_1^{e_1}p_2^{e_2}\dots p_r^{e_r}$. Now note that all divisors of n must be composed of these prime powers $\prod_{i=1}^r p_i^{a_i}$ where $a_i\in\{0,1,\dots,e_i\}$. Moreover, we note that every permutation of $a_i\in\{0,1,\dots e_i\}$ for all i must occur to create all the distinct factors of n. Therefore, we can write:

$$\sigma_k(n) = \left(1+p_1^k+p_1^{2k}+\ldots+p_1^{e_1k}\right)\left(1+p_2^k+p_2^{2k}+\ldots+p_2^{e_2k}\right)\dots\left(1+p_2^k+p_2^{2k}+\ldots+p_2^{e_2k}\right) \tag{3.1}$$

$$= \prod_{i=1}^{\omega(n)}\left(1+p_i^k+p_i^{2k}+\ldots+p_i^{e_ik}\right) \tag{3.2}$$

Where $\omega(n)$ is the number of distinct primes dividing n. Note that this particular way of writing $\sigma_k(n)$ comes about because the above multiplication runs over all the permutations of $a_i\in\{0,1,\dots,e_i\}$ for all i and therefore covers all of the divisors of n.

Now consider two integers a,b such that $(a,b)>1$. This implies that a and b share at least one prime factor p_i. This means one or more terms $p_i^{a_i}$ occur in both a and b. However, these terms $p_i^{a_i}$ occur only once in the expansion of ab. Now let there be q prime factors that are repeated, each with $a_{jk}\in\{0,1,\dots,e_j\}$. We have the following:

$$\sigma_k(ab) = \prod_{i=1}^{\omega(ab)}\left(1+p_i^k+p_i^{2k}+\ldots+p_i^{e_ik}\right) \tag{3.3}$$

$$= \left(\prod_{i=1}^{\omega(a)}\left(1+p_i^k+p_i^{2k}+\ldots+p_i^{e_ik}\right)\right)\left(\prod_{i=1}^{\omega(b)}\left(1+p_i^k+p_i^{2k}+\ldots+p_i^{e_ik}\right)\right)-\sum_{j=1}^{q}\sum_{k=0}^{e_j}p_j^{a_{jk}} \tag{3.4}$$

$$= \sigma_k(a)\sigma_k(b)-\sum_{j=1}^{q}\sum_{k=0}^{e_j}p_j^{a_{jk}} \tag{3.5}$$

Since $\sum_{j=1}^{q}\sum_{k=0}^{e_j}p_j^{a_{jk}}>0$ because there are repeated factors, we know that $\sigma_k(ab)<\sigma_k(a)\sigma_k(b)$. Moreover, since $d(n)=\sigma_0(n)$ is just a special case of $\sigma_k(n)$ where $k=0$, we have also shown that $d(ab)<d(a)d(b)$ when $(a,b)>1$. $\square$

4. Problem 4

Recall that a perfect number n is one for which $\sigma(n)=2n$.

Problem 4.1. *If $p=2^m-1$ is a prime, show that $2^{m-1}(2^m-1)$ is a perfect number.*

Solution We must show that $\sigma(2^{m-1}(2^m-1))=2^m(2^m-1)$. Since we know that $\sigma(n)$ is multiplicative, and we know that $(2^{m-1},2^m-1)=1$ because 2^m-1 is a prime, we find that:

$$\sigma(2^{m-1}(2^m-1)) = \sigma(2^{m-1})\sigma(2^m-1) \tag{4.1}$$

$$= \sigma(2^{m-1})(1+2^m-1) \tag{4.2}$$

$$= \sigma(2^{m-1})2^m \tag{4.3}$$

This follows since the only divisors of 2^m-1 are itself and 1. Next, we must compute $\sigma(2^{m-1})$. However, we know that the only divisors are powers of two. Thus, we have:

$$\sigma(2^{m-1}) = 1+2+2^2+\ldots+2^{m-1} \tag{4.4}$$

$$= \sum_{i=0}^{m-1}2^i \tag{4.5}$$

$$= \frac{2^{m-1+1}-1}{2-1} \tag{4.6}$$

$$= 2^m-1 \tag{4.7}$$

Multiplying these together, we find that $\sigma(2^{m-1}(2^m-1))=2^m(2^m-1)$, which is exactly what we wanted to show. $\square$

Problem 4.2. *Show that every even perfect number is of the form $2^{m-1}(2^m-1)$.*

Solution First, if n is an even number, then we can decompose it into $n = 2^r s$ where s is odd. We know that $\sigma(n) = \sigma(2^r)\sigma(s)$ by the multiplicative property and since $(2^r, s) = 1$. Moreover, we know that $\sigma(2^r) = \sum_{i=0}^{r} 2^i = 2^{r+1} - 1$. Therefore, we see that $\sigma(n) = (2^{r+1}-1)\sigma(s)$. However, since n is also a perfect number, we know that $\sigma(n) = 2(2^r s) = 2^{r+1}s$. We can equate these two expressions for $\sigma(n)$ and obtain:

$$(2^{r+1}-1)\sigma(s) = 2^{r+1}s \tag{4.8}$$

This shows that $2^{r+1}-1 | 2^{r+1}s$. Since it is clear that $2^{r+1}-1 \nmid 2^{r+1}$, we must have $2^{r+1}-1 | s$. This implies that we can rewrite s in the form $s = k(2^{r+1}-1)$. Substituting this back into our expression, we find:

$$(2^{r+1}-1)\sigma(s) = 2^{r+1}k(2^{r+1}-1) \tag{4.9}$$

$$\sigma(s) = 2^{r+1}k \tag{4.10}$$

However, we see that $s = k(2^{r+1}-1) = k2^{r+1} - k$. This shows that $2^{r+1}k = s + k$. Thus, we have found that $\sigma(s) = s + k$. Since $\sigma(\cdot)$ is the sum of divisors function, this can only occur when s is prime and $k = 1$. This means that $s = 2^{r+1}-1$ is a Marsenne prime. This means that $n = 2^r(2^{r+1}-1)$ is a perfect number with the form that we wanted to show. □

5. Problem 5

Problem 5.1. *For any positive integer n, let $\lambda(n) = (-1)^{\Omega(n)}$. This is the Liouville's lambda function. Show that $\lambda(n)$ is totally multiplicative and that*

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & n \text{ is a perfect square} \\ 0 & \text{otherwise} \end{cases} \tag{5.1}$$

Solution First, we shall show that $\lambda(n)$ is completely multiplicative. We know by the Fundamental Theorem of Arithmetic that $n = p_1^{e_1} \dots p_r^{e_r}$ is a unique factorization. Therefore, we know that $\Omega(n)$, the number of primes dividing n with multiplicity, is just $e_1 + e_2 + \dots + e_r$. Therefore, $\Omega(ab) = \Omega(a) + \Omega(b)$ since we can decompose a and b to be $a = \prod_{i=1}^{r} p_i^{e_{a_i}}$ and $b = \prod_{i=1}^{r} p_i^{e_{b_i}}$ such that $a_i + b_i = e_i$. This means $\Omega(a) = a_1 + a_2 + \dots + a_r$ and $\Omega(b) = b_1 + b_2 + \dots + b_r$, which shows that $\Omega(ab) = e_1 + e_2 + \dots + e_r$, which is what we wanted. Since $\Omega(n)$ is completely additive, we see that $\lambda(ab) = (-1)^{\Omega(ab)} = (-1)^{\Omega(a)+\Omega(b)} = (-1)^{\Omega(a)}(-1)^{\Omega(b)} = \lambda(a)\lambda(b)$.

Now, we shall prove the second part of the problem. First, we can decompose any number into $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$. Now, summing over all divisors of n consistitutes summing over all permutations of $p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ where $a_i \in \{0, 2, \dots, e_i\}$. Thus, we can write the sum as:

$$\sum_{d|n} \lambda(d) = \prod_{i=1}^{r} \left(\lambda(1) + \lambda(p_i) + \lambda(p_i^2) + \dots + \lambda(p_i^{e_i})\right) \tag{5.2}$$

$$= \prod_{i=1}^{r} \left(\lambda(1) + \lambda(p_i) + \lambda(p_i)^2 + \dots + \lambda(p_i)^{e_i}\right) \tag{5.3}$$

Now notice that $\lambda(1) = (-1)^{\Omega(1)} = (-1)^0 = 1$ since there are no prime divisors of 1. Moreover, there is exactly one prime divisor for every prime p_i, namely p_i. Thus, for a prime p_i, we must have $\lambda(p_i) = (-1)^1 = -1$. Knowing this, we can rewrite the above expression to:

$$\sum_{d|n} \lambda(d) = \prod_{i=1}^{r} \left(\lambda(1) + \lambda(p_i) + \lambda(p_i)^2 + \dots + \lambda(p_i)^{e_i}\right) \tag{5.4}$$

$$= \prod_{i=1}^{r} 1 + (-1) + (-1)^2 + (-1)^3 + \dots + (-1)^{e_i} \tag{5.5}$$

$$= \prod_{i=1}^{r} 1 + (-1)^{e_i} \tag{5.6}$$

Thus, if e_i is even, then the series $(-1) + (-1)^2 + \dots + (-1)^{e_i}$ telescopes to 0. If e_i is odd, the series telescopes to -1. Thus, we find:

$$\sum_{d|n} \lambda(d) = \prod_{i=1}^{r} f(e_i) \qquad \text{where } f(e_i) = \begin{cases} 0 & \text{if } e_i \text{ is odd} \\ 1 & \text{if } e_i \text{ is even} \end{cases} \tag{5.7}$$

Now we note that all e_i are even if and only if n is a perfect square. This follows because if e_i are all even, one can write n as $n = (p_1^{e_1/2} p_2^{e_2/2} \dots p_r^{e_r/2})^2$, which shows that n is a perfect square. If n is a perfect square, then each e_i must be divisible by 2 because $n = (p_1^{a_1} p_2^{a_2} \dots p_r^{a_r})^2$, so each $e_i = 2a_i$. Since $\sum_{d|n} \lambda(d) = 1$ if and only if $f(e_i) = 1$ for all i (which occurs if and only if all e_i are even), we see that the statement we wanted to prove is correct. □

6. Problem 6

Problem 6.1. *Show that*

$$\sum_{d|n} d(d)^3 = \left(\sum_{d|n} d(d) \right)^2 \tag{6.1}$$

for all positive integers n.

Solution Let $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ by the Fundamental Theorem of Arithmetic. First, we know that $d(n)$ is multiplicative so that $d(ab) = d(a)d(b)$ when $(a,b) = 1$. Namely, this means that we can expand $\sum_{d|n} d(d)$ and $\sum_{d|n} d(d)^3$ into a product of sums. We find:

$$\sum_{d|n} d(d)^3 = \prod_{i=1}^{r} d(1)^3 + d(p_i)^3 + d(p_i^2)^3 + \dots + d(p_i^{e_i})^3 \tag{6.2}$$

$$= \prod_{i=1}^{r} 1^3 + (1+1)^3 + (2+1)^3 + \dots + (e_i+1)^3 \tag{6.3}$$

$$= \prod_{i=1}^{r} \sum_{j=0}^{e_i} (j+1)^3 \tag{6.4}$$

$$= \prod_{i=1}^{r} \frac{1}{4}(e_i+1)^2(e_i+2)^2 \tag{6.5}$$

Where we have used the fact that $d(p^e) = e+1$ if p is a prime, because all of the factors of p^e are $\{1, p, p^2, \dots, p^e\}$ which contains $e+1$ elements. We have also used the fact that $(d(ab))^3 = (d(a)d(b))^3 = d(a)^3 d(b)^3$ because d is multiplicative. Next, we shall expand out the right hand side:

$$\left(\sum_{d|n} d(d) \right)^2 = \left(\prod_{i=1}^{r} d(1) + d(p_i) + d(p_i^2) + \dots + d(p_i^{e_i}) \right)^2 \tag{6.6}$$

$$= \left(\prod_{i=1}^{r} 1 + (1+1) + (2+1) + \dots + (e_i+1) \right)^2 \tag{6.7}$$

$$= \left(\prod_{i=1}^{r} \sum_{j=0}^{e_i} (j+1) \right)^2 \tag{6.8}$$

$$= \left(\prod_{i=1}^{r} \frac{1}{2}(e_i+1)(e_i+2) \right)^2 \tag{6.9}$$

$$= \prod_{i=1}^{r} \frac{1}{4}(e_i+1)^2(e_i+2)^2 \tag{6.10}$$

Clearly, these are the same, so we have finished the proof. □

7. Problem 7

Problem 7.1. *Suppose $f(n)$ is an arithmetic function whose values are all nonzero, and put $\hat{F}(n) = \prod_{d|n} f(d)$. Show that*

$$f(n) = \prod_{d|n} \hat{F}(d)^{\mu(n/d)}. \tag{7.1}$$

Solution We shall expand out the right hand side, noting that since we range over $d|n$, we can exchange d for n/d:

$$\prod_{d|n} \hat{F}(d)^{\mu(n/d)} = \prod_{d|n} \hat{F}(n/d)^{\mu(d)} \tag{7.2}$$

$$= \prod_{d|n} \left(\prod_{e|\frac{n}{d}} f(e) \right)^{\mu(d)} \tag{7.3}$$

Now this is a product of all the numbers $f(e)^{\mu(d)}$ where d and e are natural numbers with $de|n$. Thus, we can exchange the places of d and e to obtain the following expression:

$$\prod_{d|n} \hat{F}(d)^{\mu(n/d)} = \prod_{e|n} \prod_{d|\frac{n}{e}} f(e)^{\mu(d)} \tag{7.4}$$

$$= \prod_{e|n} f(e)^{\sum_{d|\frac{n}{e}} \mu(d)} \tag{7.5}$$

$$= \prod_{e|n} f(e)^{h(n/e)} \tag{7.6}$$

Where we have, by a lemma proven in class:

$$h(n/e) = \sum_{d|\frac{n}{e}} \mu(d) = \left\{ \begin{array}{ll} 1 & \text{if } n/e = 1 \\ 0 & \text{if } n/e > 1 \end{array} \right. \tag{7.7}$$

This means that $f(e)^{h(n/e)} = f(n)$ when $e = n$ and $f(e)^{h(n/e)} = 0$ otherwise. This shows that $f(n) = \prod_{d|n} \hat{F}(d)^{\mu(n/d)}$, which is what we wanted to show. □

Problem 7.2. *Show that*

$$\prod_{\substack{a=1 \\ (a,n)=1}}^{n} a = n^{\phi(n)} \prod_{d|n} \left(\frac{d!}{d^d} \right)^{\mu(n/d)} \tag{7.8}$$

Solution We know from the previous problem that if $\hat{F}(n) = \prod_{d|n} f(d)$, then $f(n) = \prod_{d|n} \hat{F}(d)^{\mu(n/d)}$. Thus, if we set $\hat{F}(d) = d!/d^d$, the proof of the problem is equivalent to proving that:

$$\frac{n!}{n^n} = \prod_{d|n} \frac{1}{d^{\phi(d)}} \prod_{\substack{a=1 \\ (a,n)=1}}^{d} a \tag{7.9}$$

We shall use the prime factorization of $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$. Clearly, all factors $d|n$ have the form $p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ where $a_i \in \{0, 1, \dots, e_i\}$. We know that the sum $\sum_{d|n} \phi(d) = n$. Moreover, we know that $d = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$. Thus, we can write $\prod_{d|n} d^{\phi(d)}$ as composed of their individual primes, exponentiated to some power. For p_i, we see that there are at least $\sum_{d|n} \phi(d) = n$ exponents, as well as some extra. Counting these, we find that p_i has the exponents:

$$p_i^{(\sum_{d|n} \phi(n))(e_i+1)e_1 e_2 \dots e_r} = p_i^{n(e_i+1)e_1 \dots e_r} \tag{7.10}$$

Substituting this back into the equation, we find that

$$\prod_{d|n} \frac{1}{d^{\phi(d)}} \prod_{\substack{a=1 \\ (a,n)=1}}^{d} a = \frac{1}{n^n} \frac{1}{p_1^{(e_1+1)\dots e_r} \dots p_r^{e_1 \dots (e_r+1)}} \prod_{d|n} \prod_{\substack{a=1 \\ (a,n)=1}}^{d} a \tag{7.11}$$

$$= \frac{n!}{n} \tag{7.12}$$

Which is what we wanted to show. □

8. Problem 8

Let f, g be airthmetic functions.

Problem 8.1. *Show that $Z(f*g,s) = Z(f,s)Z(g,s)$.*

Solution We shall expand out $Z(f*g,s)$ according to its definition:

$$Z(f*g,s) = \sum_{n\geq 1} \frac{(f*g)(n)}{n^s} \tag{8.1}$$

$$= \sum_{n\geq 1}\sum_{d|n} \frac{1}{n^s} f(n/d)g(d) \tag{8.2}$$

Now let us expand out $Z(f,s)Z(g,s)$ according to its definition:

$$Z(f,s)Z(g,s) = \left(\sum_{n\geq 1} \frac{f(n)}{n^s}\right)\left(\sum_{n\geq 1} \frac{g(n)}{n^s}\right) \tag{8.3}$$

$$= \sum_{i\geq 1} \frac{f(1)g(i)}{1^s i^s} + \sum_{i\geq 1} \frac{f(2)g(i)}{2^s i^s} + \dots \tag{8.4}$$

$$= \sum_{z\geq 1}\sum_{i\geq 1} \frac{f(z)g(i)}{z^s i^s} \tag{8.5}$$

$$= \sum_{z\geq 1}\sum_{i\geq 1} \frac{1}{(zi)^s} f(z)g(i) \tag{8.6}$$

We use a change of variables and set $n = zi$ and $d = i$. Next, we notice that i ranges over the set N, while d for $d|n$ ranges over the set $(zi)/d = (zi)/i = z$ where z ranges over N. Thus, $d|n$ ranges over N and we can rewrite the above expression as:

$$Z(f,s)Z(g,s) = \sum_{n\geq 1}\sum_{d|n} \frac{1}{n^s} f(n/d)g(d) \tag{8.7}$$

This is what we found that $Z(f*g,s)$ was equal to, so we have finished. □

Problem 8.2. *Show that there is an arithmetic function f^{-1} such that $f*f^{-1} = f^{-1}*f = 1$ if and only if $f(1) \neq 0$.*

Solution Let f be an arithmetic function such that $f(1) \neq 0$. By definition, we want to show that $(f*f^{-1})(1) = 1$ and $(f*f^{-1})(n) = 0$ for all $n > 1$. Thus, we want to find f^{-1} such that $f(1)f^{-1}(1) = 1$ and $(f*f^{-1})(n) = \sum_{d|n} f^{-1}(d)f(n/d) = 0$ for all $n > 1$. We must show that there exists a unique solution f^{-1}. First, we know that $f^{-1}(1) = 1/f(1)$ will work when $n = 1$ because $f(1) \neq 0$. Moreover, notice that this is a unique value. Now, we shall proceed to show that all $f^{-1}(n)$ are unique by induction. Suppose that there exist unique values $f^{-1}(1), f^{-1}(2), \dots f^{-1}(n-1)$. Since $f(1) \neq 0$, we can rewrite the condition that $\sum_{d|n} f^{-1}(d)f(n/d) = 0$ as the following:

$$0 = f^{-1}(n)f(1) + \sum_{d|n, d<n} f^{-1}(d)f(n/d) \tag{8.8}$$

$$f^{-1}(n) = -\frac{1}{f(1)} \sum_{d|n,d<n} f^{-1}(d)f(n/d) \tag{8.9}$$

Since each $f^{-1}(x)$ for $x < n$ were unique, we can see that $f^{-1}(n)$ must also be unique.

To show the converse, we note that if $f^{-1}(n)$ exists, then it must be of the form $f^{-1}(n) = -\frac{1}{f(1)}\sum_{d|n,d<n} f^{-1}(d)f(n/d)$ since we have just shown that this inverse is unique. Since this exists and is well defined, we know that $f(1) \neq 0$. This completes the proof. □