18.781 Solutions to Problem Set 6

1. Since both sides are positive, it's enough to show their squares are the same. Now $\prod_{d|n} d = \prod_{d|n} \frac{n}{d}$, so

$$\begin{aligned}\left(\prod_{d|n} d\right)^2 &= \left(\prod_{d|n} d\right)\left(\prod_{d|n} \frac{n}{d}\right)\\ &= \prod_{d|n} d \cdot \frac{n}{d}\\ &= \prod_{d|n} n\\ &= n^{d(n)}.\end{aligned}$$

2. For a prime power p^e, we have
$$\sigma_k(p^e) = 1 + p^k + \cdots + p^{ek},$$
which is odd if and only if $p = 2$ or e is even. So if $n = p_1^{e_1} \cdots p_r^{e_r}$, then
$$\sigma_k(n) = \prod_{i=1}^{r} \sigma_k(p_i^{e_i})$$
is odd if and only if all the odd primes dividing n divide it to an even power, i.e., n is a square or twice a square.

3. Suppose $g = \gcd(a, b) > 1$, and let $S(n) = \{d \in \mathbb{N} : d|n\}$ be the set of all positive divisors of n. We have a function $\phi : S(a) \times S(b) \to S(ab)$ given by $\phi(d, e) = de$. The map ϕ is surjective, but not injective, because $\phi(g, 1) = \phi(1, g)$. So

$$\begin{aligned}\sigma_k(ab) &= \sum_{x \in S(ab)} x^k\\ &< \sum_{t \in S(a)\times S(b)} \phi(t)^k\\ &= \left(\sum_{d|a} d^k\right)\left(\sum_{e|b} e^k\right)\\ &= \sigma_k(a)\sigma_k(b).\end{aligned}$$

Similarly, $d(ab) < d(a)d(b)$ just says $|S(ab)| < |S(a)||S(b)|$, which is obvious from the fact that ϕ is surjective but not injective, or from noting that $d(n) = \sigma_0(n)$.

4. (a) If $2^m - 1$ is prime then $\sigma(2^m - 1) = 2^m$. Since $\sigma(2^{m-1}) = 1 + 2 + \cdots + 2^{m-1} = 2^m - 1$, if $n = 2^{m-1}(2^m - 1)$, then we have
$$\sigma(n) = \sigma(2^{m-1})\sigma(2^m - 1) = (2^m - 1)2^m = 2n.$$
So n is perfect.

(b) Suppose n is perfect and even. Write $n = 2^r s$ where $r \geq 1$ and s is odd. It's easy to rule out $s = 1$, so we'll assume $s > 1$. Then $\sigma(n) = (2^{r+1} - 1)\sigma(s)$ must equal $2n = 2^{r+1}s$. So $2^{r+1} - 1$ divides $2^{r+1}s$, and since $\gcd(2^{r+1} - 1, 2^{r+1}) = 1$, we have $2^{r+1} - 1 \mid s$.

Now if $s > 2^{r+1} - 1$, then s has at least the three divisors $1, s$, and $s/(2^{r+1} - 1)$, which are distinct because $r \geq 1$. Thus

$$\sigma(s) \geq 1 + s\left(1 + \frac{1}{2^{r+1} - 1}\right) > s\left(\frac{2^{r+1}}{2^{r+1} - 1}\right),$$

so $(2^{r+1} - 1)\sigma(s) > 2^{r+1}s$, contradiction. Therefore we must have $s = 2^{r+1} - 1$, and $\sigma(s) = 2^{r+1}$. But $s = 2^{r+1} - 1$ has at least the two divisors 1 and s, which sum to 2^{r+1} already. So the only possibility is that these are the only two divisors of s, i.e., s is prime.

5. The function $\Omega(n)$ is the number of primes dividing n, with multiplicity, so $\Omega(mn) = \Omega(m) + \Omega(n)$ for any m, n. Hence $\lambda(n)$ is totally multiplicative, and $\sum_{d|n} \lambda(d)$ is multiplicative (but not totally multiplicative). For prime powers p^e,

$$\begin{aligned}\sum_{d|p^e} \lambda(d) &= \underbrace{1 + (-1) + 1 + (-1) + \cdots + (-1)^e}_{(e+1) \text{ terms}} \\ &= \begin{cases} 0 & \text{if e is odd,} \\ 1 & \text{if e is even.} \end{cases}\end{aligned}$$

So for $n = p_1^{e_1} \cdots p_r^{e_r}$, $\sum_{d|n} \lambda(d)$ will be 0 if any of the e_i are odd, and 1 if all of the e_i are even (which occurs precisely when n is a perfect square).

6. Both sides are multiplicative, so it's enough to show the equality for prime powers p^e. Since $1^3 + \cdots + n^3 = \frac{n^2(n-1)^2}{4}$, as can be easily proven using induction,

$$\begin{aligned}\sum_{d|p^e} d(d)^3 &= \sum_{i=0}^{e} d(p^i)^3 \\ &= \sum_{i=0}^{e} (i+1)^3 \\ &= \frac{e^2(e+1)^2}{4} \\ &= \left(\sum_{i=1}^{e+1} i\right)^2 \\ &= \left(\sum_{d|p^e} d(d)\right)^2.\end{aligned}$$

7. (a) This is just a multiplicative version of the Möbius inversion formula. To prove it we use the fact that

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1. \end{cases} \qquad (*)$$

So

$$\begin{aligned}\prod_{d|n} \hat{F}(d)^{\mu(n/d)} &= \prod_{d|n} \left(\prod_{e|d} f(e) \right)^{\mu(n/d)} \\ &= \prod_{\substack{e,f \\ ef|n}} f(e)^{\mu(n/ef)} \\ &= \prod_{e|n} f(e)^{\sum_{f|m} \mu(m/f)},\end{aligned}$$

where $m = n/e$. By $(*)$, this expression is simply $f(n)$.

(b) Writing this equation as

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

we see that by part (a) it's enough to show that

$$\prod_{d|n} f(d) = \frac{n!}{n^n}$$

where

$$f(n) = \prod_{\substack{a=1 \\ (a,n)=1}}^{n} \left(\frac{a}{n} \right)$$

is the left-hand side.

Now $\frac{n!}{n^n}$ is the product over $x \in \{1, \ldots, n\}$ of $\frac{x}{n}$. For any such x, let $g = \gcd(x, n)$. Then the fraction $\frac{x}{n}$ is reduced to $\frac{x/g}{n/g}$. Conversely, for any divisor n' of n and any $x' \in \{1, \ldots, n'\}$ coprime to n', we have $\frac{x'}{n'} = \frac{x'n/n'}{n}$, where $x'n/n' \in \{1, \ldots, n\}$ has gcd exactly $g = n/n'$ with n. Therefore,

$$\begin{aligned}\frac{n!}{n^n} &= \prod_{n'|n} \left(\prod_{\substack{x'=1 \\ (x',n')=1}}^{n'} \frac{x'}{n'} \right) \\ &= \prod_{n'|n} f(n'),\end{aligned}$$

which is what we set out to prove.

8. (a) We have

$$\begin{aligned}Z(f,s)Z(g,s) &= \left(\sum_{m \geq 1} \frac{f(m)}{m^s} \right) \left(\sum_{n \geq 1} \frac{g(n)}{n^s} \right) \\ &= \sum_{m,n \geq 1} \frac{f(m)g(n)}{(mn)^s},\end{aligned}$$

which, when recast as a sum over $mn = k$, becomes

$$\sum_{k \geq 1} \frac{\sum_{m|k} f(m)g(k/m)}{k^s} = Z(f * g, s).$$

(b) First suppose f has an inverse $g = f^{-1}$. Then

$$(f * g)(1) = f(1)g(1) = 1,$$

so $f(1) \neq 0$.

Conversely, when $f(1) \neq 0$, we will construct a function g such that $f * g = \mathbf{1}$. First set $g(1) = f(1)^{-1}$, which is forced as above. Now we will define $g(n)$ for all n, by induction on n. The base case $n = 1$ is done. Suppose $g(n)$ has been defined for all n less than k. Then we have

$$\begin{aligned}
0 &= \mathbf{1}(k) \\
&= (f * g)(k) \\
&= \sum_{d|k} f(d)g(k/d) \\
&= f(1)g(k) + \sum_{d|k, d>1} f(d)g(k/d).
\end{aligned}$$

All the $g(k/d)$ for $d > 1$ have been defined, by the inductive hypothesis, so we can solve this equation uniquely for $g(k)$. This completes the induction. By construction, $f * g = \mathbf{1}$, and by commutativity of $*$ we also have $g * f = \mathbf{1}$.

9. (a) This is a standard proof by induction.

(b) Splitting the integers from 1 through n by their gcd d with n, we get

$$\begin{aligned}
\sum_{j=1}^{n} j^2 &= \sum_{d|n} \sum_{(j,n)=d} j^2 \\
&= \sum_{d|n} d^2 S(n/d) \\
&= \sum_{d|n} \frac{n^2}{d^2} S(d).
\end{aligned}$$

(c) Note that

$$n^2 \sum_{d|n} \frac{S(d)}{d^2} = \sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}.$$

Therefore,

$$\sum_{d|n} \frac{S(d)}{d^2} = \frac{1}{6}\left(2n + 3 + \frac{1}{n}\right),$$

and Möbius inversion gives

$$\frac{S(n)}{n^2} = \sum_{d|n} \frac{1}{6}\mu(d)\left(\frac{2n}{d} + 3 + \frac{d}{n}\right).$$

(d) Since the LHS and RHS are both multiplicative, it's enough to show equality for prime powers p^e. In this case

$$\sum_{d|p^e} d\mu(d) = 1 - p$$

and

$$(-1)^{\omega(p^e)}\phi(p^e)\frac{s(p^e)}{p^e} = (-1)p^{e-1}(p-1)\frac{p}{p^e} = 1 - p.$$

(e) As shown in part (c),

$$\frac{S(n)}{n^2} = \frac{1}{3}\sum_{d|n}\mu(d)\frac{n}{d} + \frac{1}{2}\sum_{d|n}\mu(d) + \frac{1}{6n}\sum_{d|n}\mu(d)d.$$

Now, for any n, $\sum_{d|n}\mu(d)\frac{n}{d} = \phi(n)$. Also, $\sum_{d|n}\mu(d) = \mathbf{1}(n)$. So when $n > 1$, we get

$$S(n) = \frac{n^2\phi(n)}{3} + \frac{(-1)^{\omega(n)}\phi(n)s(n)}{6}.$$

10. (a) This follows from the Multiplicative version of Möbius inversion, using $f(n) = \Phi_n(x)$ and $x^n - 1 = \prod_{d|n}\Phi_n(x) = F(n)$.

(b) $F(n)$ is the sum of the roots of the polynomial $x^n - 1$, so it's equal to the negative of the coefficient of x^{n-1} in $x^n - 1$. Therefore

$$F(n) = \begin{cases} 0 & \text{if } n > 1 \\ 1 & \text{if } n = 1. \end{cases}$$

(c) Since

$$\prod_{d|n}\Phi_d(x) = x^n - 1,$$

the sum of the roots of the polynomial $x^n - 1$ is

$$F(n) = \sum_{d|n} f(d),$$

where

$$f(d) = \sum_{\substack{a=1 \\ (a,n)=1}}^{n} e^{2\pi i a/n}$$

is the sum of the roots of $\Phi_d(x)$. Therefore, $f * U = \mathbf{1}$, so by Möbius inversion $f = \mu$.

18.781 Theory of Numbers
Spring 2012