Geoffrey Thomas
18.781 pset 8
Collaborators: Liz Denys

4.1 15. Define k as the unique integer satisfying $\frac{k}{n} \leq \xi < \frac{k+1}{n}$. Note that $[\xi] = \left[\frac{k}{n}\right]$, since $n[\xi] = k$. Therefore we can write the summation as

$$\left[\frac{k}{n}\right] + \left[\frac{k+1}{n}\right] + \cdots + \left[\frac{k+n-1}{n}\right]$$

Write $k = qn + r$ where q, r are integers and $0 \leq r < n$. Then the summation becomes

$$\left[\frac{qn+r}{n}\right] + \left[\frac{qn+r+1}{n}\right] + \cdots + \left[\frac{(q+1)n+r-1}{n}\right]$$

The first $(n-r)$ terms of this summation, $\left[\frac{qn+r}{n}\right]$ through $\left[\frac{qn+(n-1)}{r}\right]$, all equal q. The remaining r terms, $\left[\frac{(q+1)n}{n}\right]$ through $\left[\frac{(q+1)n+r-1}{n}\right]$, all equal $q+1$. Therefore the summation is $q(n-r) + (q+1)r = qn + 1$. Meanwhile, the right hand side of the equation is $[n\xi] = [k] = k = qn + 1$, so the equation holds.

4.1 21. WLOG let u, v be positive so we can safely take principal square roots. From the stipulation $u - v \leq \sqrt[4]{64n}$,

$$\begin{aligned}
(u+v)^2 - (u-v)^2 &= 4uv \\
(u+v)^2 - \sqrt{64uv} &\leq 4uv \\
(u+v)^2 &\leq 4uv + 8\sqrt{uv} \\
\frac{(u+v)}{2} &\leq \sqrt{uv + 2\sqrt{uv}} \leq \sqrt{uv + 2\sqrt{uv} + 1} = \sqrt{\left(\sqrt{uv}+1\right)^2} = \sqrt{uv} + 1
\end{aligned}$$

Meanwhile,

$$\begin{aligned}
4uv &= (u+v)^2 - (u-v)^2 \\
4uv &< (u+v)^2 \\
\sqrt{uv} &< \frac{(u+v)}{2}
\end{aligned}$$

Now $u + v$ is even because u and v are both factors of an odd integer (and so are both odd), and so $\frac{(u+v)}{2}$ is an integer. The two results bound $\frac{(u+v)}{2}$ to a unique integer, specifically $[\sqrt{uv} + 1]$. Therefore, the equation in question is $x^2 - (u+v)x + uv$, whose roots are u and v, both of which are positive integers.

4.2 5. Represent $n = \prod_p^{\alpha}$. Then consider $\prod_{d|n} d$ in the form $\prod_p p^{\beta}$. For a given p, the divisors of n are the divisors of $\frac{n}{p^{\alpha}}$ times all possible powers of p, 1 through α. So the power of p is given by the sum of the possible powers of p in n times the number of divisors of $\frac{n}{p^{\alpha}}$, i.e., $\beta = \frac{1}{2}\alpha(\alpha+1)\frac{d(n)}{\alpha+1} = \frac{d(n)}{2}\alpha$, so $\prod_{d|n} d = \prod_p p^{\frac{d(n)}{2}\alpha} = \prod_p p^{\alpha\frac{d(n)}{2}} = n^{\frac{d(n)}{2}}$.

4.2 15. Since σ_k is multiplicative, it suffices to show this for prime powers, since then $\sigma_k\left(p^{a_1}q^{a_2}p^{b_1}q^{b_2}\right) = \sigma_k\left(p^{a_1b_1}\right)\sigma_k\left(q^{a_2b_2}\right) < \sigma_k\left(p^{a_1}\right)\sigma_k\left(p^{b_1}\right)\sigma_k\left(q^{a_2}\right)\sigma_k\left(q^{b_2}\right) = \sigma_k\left(p^{a_1}q^{a_2}\right)\sigma_k\left(p^{b_1}q^{b_2}\right)$, and similarly for more prime factors.

Let $a = p^n$ and $b = q^m$ for primes p, q and for n, m positive integers. Since $(a, b) > 1$, it follows that $p = q$. $\sigma_k\left(p^{nm}\right) = 1+p^k+\cdots+\left(p^k\right)^{nm}$. $\sigma_k\left(p^n\right)\sigma_k\left(p^m\right) = \left(1+p^k+\cdots+\left(p^k\right)^n\right)\left(1+p^k+\cdots+\left(p^k\right)^n\right)$, which expands to a polynomial of p^k whose first and last terms have coefficient 1, but with all middle terms having greater coefficients. Therefore the second expression is greater than the first.

4.2 16. If $2^n - 1$ is prime, then the sum of the divisors of $2^{n-1}\left(2^n-1\right)$ is $\left(2^n-1\right)\left(1+2^n-1\right) = 2^n\left(2^n-1\right) = 2p$. Since 3, 7, and 31 are primes of the form $2^n - 1$, we can say that 6, 28, and 496 are perfect.

4.2 19. If x is an even perfect number, then $x = 2^{a-1}b$ for some $a \geq 2$ and odd $b \geq 3$. The sum of its divisors is $\left(2^a-1\right)\sigma(b) = 2^a b$ by definition. Since $2^a - 1 \not| 2^a$, $b = c\left(2^a-1\right)$ for some integer c. So, again, we have $\left(2^a-1\right)\sigma(b) = 2^a c\left(2^a-1\right)$. Cancelling, we have $\sigma(b) = 2^a c$. Since $\sigma(b)$ is the sum of all divisors, we know that $\sigma(b) \geq c\left(2^a-1\right)+c = c2^a$. But we previously found that this is an equality, so there must be no other divisors — i.e., $c = 1$, and $b = c\left(2^a-1\right) = 2^a - 1$ is prime, as we wanted to show.

4.2 20. $\Omega(n)$ is totally multiplicative, so $\lambda(n)$ is too, since $\lambda(ab) = (-1)^{\Omega(a)\Omega(b)} = (-1)^{\Omega a}(-1)^{\Omega b} = \lambda(a)\lambda(b)$.

By theorem 4.4, $\sum_{d|n}\lambda d$ is also multiplicative, so we can just consider prime powers. $\sum_{d|p^a}\lambda p^a = \sum_{i=1}^{a}(-1)^i$, which is 1 if a is even and 0 if a is odd, that is, 1 if p^a is a perfect square and 0 otherwise. Since the property of being a perfect square is also multiplicative, the claim holds.

4.2 24. $f(x)^n$ is multiplicative if $f(x)$ is; this, plus theorem 4.4, plus $d(n)$ being multiplicative tells us that both sides of this equation are multiplciative. So we only need show that for prime powers,

$$\sum_{d|p^a} d(d)^3 = \left(\sum_{d|p^a} d(d)\right)^2$$

$$\sum_{i=1}^{a} i^3 = \left(\sum_{i=1}^{a} i\right)^2$$

which is a known fact about summations of natural numbers.

4.

$$\begin{aligned}(f*(g*h))(n) &= \sum_{d_1|n} f(d_1)(g*h)\left(\frac{n}{d_1}\right) \\ &= \sum_{d_1|n} f(d_1)\left(\sum_{d_2|\left(\frac{n}{d_1}\right)} g(d_2)h\left(\frac{n}{d_1 d_2}\right)\right) \\ &= \sum_{\substack{d_1 d_2 d_3 = n \\ d_1,d_2,d_3 \geq 1}} f(d_1)g(d_2)h(d_3)\end{aligned}$$

since iterating through all divisors d_1 of n, all remaining divisors d_2, and the final quotient in order is the same as iterating through all d_1, d_2, d_3 that multiply to n.

Similarly,

$$\begin{aligned}((f*g)*h)(n) &= \sum_{d_3|n} (f*g)\left(\frac{n}{d_3}\right)h(d_3) \\ &= \sum_{d_3|n}\left(\sum_{d_1|\left(\frac{n}{d_3}\right)} f(d_1)g\left(\frac{n}{d_1 d_3}\right)\right)h(d_3) \\ &= \sum_{\substack{d_1 d_2 d_3 = n \\ d_1,d_2,d_3 \geq 1}} f(d_1)g(d_2)h(d_3)\end{aligned}$$

Since both orders produce the same result, the convolution operator is associative.

5.

$$\begin{aligned}Z(f*g,s) &= \sum_{n=1}^{\infty} \frac{(f*g)(n)}{n^s} \\ &= \sum_{n=1}^{\infty} \frac{\sum_{a|n} f(a)g(\frac{n}{a})}{n^s} \\ &= \sum_{n=1}^{\infty}\sum_{a|n} \frac{f(a)g(\frac{n}{a})}{n^s} \\ &= \sum_{a=1}^{\infty}\sum_{b=1}^{\infty} \frac{f(a)g(b)}{(ab)^s} \qquad (1) \\ &= \sum_{a=1}^{\infty}\sum_{b=1}^{\infty} \frac{f(a)}{a^s}\frac{g(b)}{b^s} \\ &= \left(\sum_{a=1}^{\infty}\frac{f(a)}{a^s}\right)\left(\sum_{b=1}^{\infty}\frac{g(b)}{b^s}\right) \\ &= Z(f,s)Z(g,s)\end{aligned}$$

At equation (1), we note that we can write n from the left summation in the form ab for each of its divisors a (in fact, this is the form we've written it in in the previous step, as a and n/a). Enumerating these by all integers a times all integers b is valid, since this will generate all factorizations ab of every integer (by closure of multiplication and factoring), no more, no less. So we can change variables at this point.

For the second part of this problem, we note that since we want $1 = (f*f^{-1})(1) = f(1)f^{-1}(1)$, $f(1)$ cannot be zero, proving one direction of the iff. For the other direction, we can build up each value of $f^{-1}(n)$ given $f(n)$. We have already determined $f^{-1}(1)$. We then can proceed by induction, since $f^{-1}(2)$ is the only as-yet-unconstrained value in the constraint $0 = (f * f^{-1})(2) = f(1)f^{-1}(2) + f(2)f^{-1}(1)$, and once we constrain it we can do the same for higher values of n in $f^{-1}(n)$. Specifically, with strong induction, we have for any n

$$\begin{aligned} 0 =& \sum_{d|n} f\left(\frac{n}{d}\right) f^{-1}(d) \\ =& f(1)f^{-1}(n) + \sum_{d|n,\, d\neq n} f\left(\frac{n}{d}\right) f^{-1}(d) \end{aligned}$$

where the summation in the second line only includes f^{-1} of proper divisors of n, and the other term multiplies the unknown $f^{-1}(n)$ by a nonzero coefficient. So this unknown can be calculated provided you know f^{-1} of its proper divisors, which given the base case of $f^{-1}(1) = f(1)^{-1}$ completes the determination of $f^{-1}(n) \forall n \in Z^+$.