Fall 2021 – Math 328K – 55385

Homework 9 Solutions

due Thursday, November 4, 14:00

Problem 1. Which positive integers m have exactly 3/4/5 positive divisors?

Solution 1. Let $m = p_1^{i_1} \cdots p_k^{i_k}$ with $p_1, \ldots, p_k$ distinct primes and $i_1, \ldots, i_k \geq 1$. Then $\tau(m) = (i_1 + 1) \cdots (i_k + 1)$.

Since 3 and 5 are prime, $\tau(m) = 3$ or $\tau(m) = 5$ implies that this product can only have one factor, so m is a prime power. Since $\tau(p^k) = k + 1$, The integers with exactly 3 positive divisors are squares of primes, and the integers with exactly 5 positive divisors are fourth powers of primes. The first 10 examples of each are:

$$4, 9, 25, 49, 121, 169, 289, 361, 529, 841$$

$$16, 81, 625, 2401, 14641, 28561, 83521, 130321, 279841, 707281$$

If $\tau(m) = 4$ there are two possibilities: either m is a prime power as before, then m has to be the cube of a prime, or m has two different prime factors, both with exponent 1. The positive integers with exactly 4 positive divisors are therefore cubes of primes and products of two different primes. The first 10 examples are:

$$6, 8, 10, 14, 15, 21, 22, 26, 27, 33$$

Problem 2. Let

$$\mathcal{F} = \{\text{functions } f \colon \mathbb{Z}_+ \to \mathbb{R}\}$$

be the set of all real valued arithmetic functions. We want to define two binary operations on $\mathcal{F}$, an addition $+$ and a multiplication $\star$. The operation $+$ is the pointwise addition of functions, defined by

$$(f + g)(n) = f(n) + g(n),$$

for any $f, g \in \mathcal{F}$ and $n \in \mathbb{Z}_+$, and $f \star g$ is the *Dirichlet product*

$$(f \star g)(n) = \sum_{d|n} f(d)g(n/d).$$

Prove the following statements, for $f, g \in \mathcal{F}$.

a) $\mathcal{F}$ with the addition $+$ and multiplication $\star$ is a commutative ring.

   Hint: as multiplicative identity, take the arithmetic function ι defined by $\iota(1) = 1$ and $\iota(n) = 0$ for all $n > 1$.

b) $f \in \mathcal{F}^\times$ if and only if $f(1) \neq 0$.

c) If f and g are multiplicative, then $f \star g$ is multiplicative.

d) If f is multiplicative and invertible, then f^{-1} is multiplicative.

e) Let $\nu \in \mathcal{F}$ be the constant function $\nu(n) = 1$. Then the inverse of ν is the Möbius function μ (that is, the multiplicative function defined by $\mu(p) = -1$ and $\mu(p^k) = 0$ for every prime number p and $k \geq 2$).

f) Let f be an arithmetic function and F its summatory function. Then $F = f \star \nu$ and $f = F \star \mu$. This is the *Möbius inversion formula.* If F is multiplicative, then f is multiplicative.

Solution 2.

a) There are many ring axioms, but most are easy to check. The interesting ones are the commutative and associative properties and the neutral element for multiplication: $f \star g = g \star f$, $f \star (g \star h) = (f \star g) \star h$, and $f \star \iota = f$ for all $f, g, h \in \mathcal{F}$.

   The commutative property just follows from the fact that

$$\{d \mid d \geq 1 \text{ divides } n\} = \{\tfrac{n}{d} \mid d \geq 1 \text{ divides } n\}.$$

   Because of this

$$(f \star g)(n) = \sum_{d|n} f(d)g(n/d) = \sum_{d|n} f(n/d)g(d) = (g \star f)(n)$$

   for all $f, g \in \mathcal{F}$ and $n \in \mathbb{Z}_+$.

   For the associative property we need to check the equality of

$$((f \star g) \star h)(n) = \sum_{d|n} \sum_{d'|d} f(d')g(\tfrac{d}{d'})h(\tfrac{n}{d})$$

   and

$$(f \star (g \star h))(n) = \sum_{d|n} \sum_{d'|\frac{n}{d}} f(d)g(d')h(\tfrac{n}{dd'}).$$

   In both cases, the summation can be rewritten as

$$\sum_{abc=n} f(a)g(b)h(c)$$

where we sum over all triples of positive integers (a,b,c) with $abc = n$.

Finally

$$(f \star \iota)(n) = \sum_{d|n} f(d)\iota(\tfrac{n}{d}) = f(n)$$

where the last equality comes from the observation that all terms in the sum vanish except when $n/d = 1$, that is $d = n$.

b) First assume $f \in \mathcal{F}^\times$. Then there is a function f^{-1} such that $f \star f^{-1} = \iota$. Evaluating at 1, we get

$$1 = \iota(1) = \sum_{d|1} f(d) f^{-1}(1/d) = f(1)f^{-1}(1).$$

So $f(1) \neq 0$ and $f^{-1}(1) = 1/f(1)$.

Conversely, assume that $f(1) \neq 0$. We want to construct a function g such that $g(1) = 1/f(1)$ and

$$\sum_{d|n} f(d)g(n/d) = 0 \qquad (\triangle)$$

for all $n \geq 2$. We can rearrange $(\triangle)$ to a recursive definition of g: First set $g(1) = 1/f(1)$. For $n \geq 2$, assume $g(k)$ is already defined for all $k < n$ and set

$$g(n) = -\frac{1}{f(1)} \sum_{d|n, d\neq 1} f(d)\, g(n/d).$$

If g is defined this way, it clearly satisfies $(\triangle)$, so $f \star g = \iota$.

c) Let f and g be multiplicative and m and n be coprime. Then

$$(f \star g)(mn) = \sum_{d|mn} f(d)g(\tfrac{mn}{d}) = \sum_{d_1|m}\sum_{d_2|n} f(d_1d_2)g(\tfrac{mn}{d_1d_2}) = \sum_{d_1|m} f(d_1)g(\tfrac{m}{d_1}) \sum_{d_2|n} f(d_2)g(\tfrac{n}{d_2})$$

$$= (f \star g)(m) \cdot (f \star g)(n).$$

We can split the sum this way by the argument we discussed in class (Lemma 7.5).

d) We can do this by induction, with the induction hypothesis for $N \in \mathbb{N}$: "$f^{-1}(mn) = f^{-1}(m)f^{-1}(n)$ for all pairs of coprime positive integers m, n with $mn \leq N$."

In the case $N = 1$ this is easy to check: the only pair m, n with $mn \leq 1$ is $m = n = 1$. Since f is multiplicative and not constant 0, we have $f(1) = 1$, and also $f^{-1}(1) = 1/f(1) = 1$. This implies $f^{-1}(1 \cdot 1) = f^{-1}(1)f^{-1}(1)$.

Now assume that the induction hypothesis has been proved for $N-1$, and let $m, n \in \mathbb{Z}_+$ be coprime with $2 \leq mn \leq N$. Then

$$0 = \iota(mn) = \sum_{d|mn} f(d) f^{-1}(\tfrac{mn}{d}) = \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2) f^{-1}(\tfrac{m}{d_1} \tfrac{n}{d_2}).$$

and also

$$0 = \iota(m)\iota(n) = \sum_{d_1|m} f(d_1) f^{-1}(\tfrac{m}{d_1}) \sum_{d_2|n} f(d_2) f^{-1}(\tfrac{n}{d_2}) = \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2) f^{-1}(\tfrac{m}{d_1}) f^{-1}(\tfrac{n}{d_2})$$

We subtract these two equations. By the induction hypothesis we have the equality $f^{-1}(\frac{m}{d_1} \frac{n}{d_2}) = f^{-1}(\frac{m}{d_1}) f^{-1}(\frac{n}{d_2})$ in all summands except when $d_1 = d_2 = 1$, so all of these terms vanish. What remains is

$$f^{-1}(mn) - f^{-1}(m) f^{-1}(n) = 0,$$

which completes the inductive step and the proof that f^{-1} is multiplicative.

e) Let p be a prime and $k \geq 1$. Then

$$(\mu \star \nu)(p^k) = \sum_{d|p^k} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^k) = 1 - 1 = 0 = \iota(p^k).$$

So $\mu \star \nu$ and ι agree on prime powers. Also, $\mu \star \nu$ is multiplicative by c) and ι is multiplicative by definition. If multiplicative functions agree on all prime powers, they are equal. So $\mu \star \nu = \iota$, or equivalently $\nu^{-1} = \mu$.

f) It is clear from the definitions of the Dirichlet product and the summatory function that $f \star \nu = F$. So

$$F \star \mu = (f \star \nu) \star \mu = f \star (\nu \star \mu) = f \star \iota = f.$$

Using c) and the multiplicativity of μ this also shows that if F is multiplicative, then f is multiplicative.

Also note that $\mu \star \nu = \iota$, $\iota \star \nu = \nu$, and $\nu \star \nu = \tau$, so we have the "sequence of summatory functions"

$$\mu \to \iota \to \nu \to \tau.$$