Elementary Number Theory - Exercise 3b

ETH Zürich - Dr. Markus Schwagenscheidt - Spring Term 2023

Problem 1. Let $\mathbf{1}(n) = 1$ be the constant 1-function, $\mathrm{id}(n) = n$ the identity, and $e(n) = 1$ for $n = 1$ and $e(n) = 0$ for $n > 1$. Compute the following Dirichlet convolutions,

$$\mathbf{1} * \mathbf{1}, \qquad \mathbf{1} * \mathrm{id}, \qquad \mathbf{1} * e, \qquad \mathrm{id} * \mathrm{id}.$$

Solution 1.

1. $(\mathbf{1} * \mathbf{1})(n) = \sum_{d|n} 1 = \tau(n)$, the number-of-divisors function.
2. $(\mathbf{1} * \mathrm{id})(n) = \sum_{d|n} d = \sigma(n)$, the sum-of-divisors function.
3. $(\mathbf{1} * e)(n) = \sum_{d|n} e(d) = \begin{cases} 1, & n = 1, \\ 0, & n > 1 \end{cases} = e(n)$.
4. $(\mathrm{id} * \mathrm{id})(n) = \sum_{d|n} d\frac{n}{d} = n \sum_{d|n} 1 = n\tau(n)$.

Problem 2. Let $\tau(n) = \sum_{d|n} 1$ be the number-of-divisors function and $\sigma(n) = \sum_{d|n} d$ the sum-of-divisors function, and let φ Euler's totient function. Show that

$$\sum_{d|n} \tau\left(\frac{n}{d}\right)\varphi(d) = \sigma(n).$$

Hint: Use that $\varphi * \mathbf{1} = \mathrm{id}$ and convolute with $\mathbf{1}$.

Solution 2. We showed in the lecture that $\sum_{d|n} \varphi(d) = n$, which means that $\varphi * \mathbf{1} = \mathrm{id}$. We convolute with $\mathbf{1}$ on both sides to get

$$\varphi * \mathbf{1} * \mathbf{1} = \mathrm{id} * \mathbf{1}.$$

We have seen in the first problem that

$$\mathbf{1} * \mathbf{1} = \tau \qquad \text{and} \qquad \mathrm{id} * \mathbf{1} = \sigma,$$

so we obtain

$$\varphi * \tau = \sigma,$$

which is the stated formula.

Problem 3. Let

$$\varphi(n) = \#\{1 \leq k \leq n \mid \gcd(k, n) = 1\}$$

be Euler's totient function.

1. Show that, if $n = p^m$ is a power of a prime, then

$$\varphi(p^m) = p^{m-1}(p-1).$$

   Hint: Count the elements $1 \leq k \leq p^m$ which are *not* coprime to p.

2. We know from the lecture that φ is multiplicative. Conlude that $\varphi(n)$ is given by

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

where the product runs over the prime divisors of n.

Solution 3. 1. We need to count the numbers $1 \le k \le p^m$ with $\gcd(k, p^m) = 1$. Equivalently, this number is given by p^m (*all* numbers $1 \le k \le p^m$) minus the number of those $1 \le k \le p^m$ with $\gcd(k, p^m) > 1$. The latter condition means that k is divisible by p, so k is of the form $k = p\ell$ for some $\ell \in \mathbb{Z}$. Since $1 \le k \le p^m$, the only possibilities for k are

$$p,\ 2p,\ 3p,\ \ldots, p^{m-1} \cdot p = p^m,$$

and those are p^{m-1} numbers. Hence we obtain

$$\varphi(p^m) = p^m - p^{m-1} = p^{m-1}(p-1)$$

2. We have seen in the lecture that φ is multiplicative. Now, using the formula for $\varphi(p^m)$ from the first item, we obtain

$$\varphi(n) = \varphi(p_1^{\nu_1} \cdots p_r^{\nu_r}) = \prod_{j=1}^{r} \varphi(p_j^{\nu_j}) = \prod_{j=1}^{r} p_j^{\nu_j}(1-1/p_j) = \prod_{j=1}^{r} p_j^{\nu_j} \cdot \prod_{j=1}^{r}(1-1/p_j) = n \prod_{p|n}(1-1/p).$$

Problem 4. Show that, for a *completely* multiplicative number-theoretic function $f \neq 0$, the inverse $\hat{f}$ with respect to convolution is given by

$$\hat{f}(n) = \mu(n) f(n), \qquad n \in \mathbb{N}.$$

Solution 4. We need to check that $f * \hat{f} = e$, where $e(1) = 1$ and $e(n) = 0$ for $n > 1$. Since f is strictly multiplicative, we can compute

$$(f * \hat{f})(n) = \sum_{d|n} f\left(\frac{n}{d}\right) \hat{f}(d) = \sum_{d|n} f\left(\frac{n}{d}\right) f(d)\mu(d) = f(n) \sum_{d|n} \mu(d),$$

which equals $f(1) = 1$ if $n = 1$, and 0 if $n > 1$ since $\sum_{d|n} \mu(d) = 0$ in this case.

Problem 5. 1. Show that

$$\varphi(n) = (\mu * \mathrm{id})(n) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

Hint: Apply the Möbius inversion formula to the summatory function of φ.

2. Show that the inverse $\hat{\varphi}$ of φ with respect to convolution is given by

$$\hat{\varphi}(n) = \sum_{d|n} \mu(d) d = \prod_{p|n} (1 - p).$$

Hint: We have $\hat{\varphi} = \hat{\mu} * \hat{\mathrm{id}}$ by the first item. What are $\hat{\mu}$ and $\hat{\mathrm{id}}$?

Solution 5. 1. We have seen in the lecture that the summatory function of φ is the identity function $\mathrm{id}(n) = n$, i.e.

$$\varphi * \mathbf{1} = \mathrm{id}.$$

By the Möebius inversion formula, we have

$$\varphi(n) = (\mathrm{id} * \mu)(n) = \sum_{d|n} \mu(n/d)d.$$

2. Since $\varphi = \mu * \mathrm{id}$ by the last item, we have $\hat{\varphi} = \hat{\mathrm{id}} * \hat{\mu}$. Now id is strictly multiplicative, so by the first item we have

$$\hat{\mathrm{id}}(n) = \mu(n)n.$$

Moreover, we have seen that the inverse of μ is the constant 1-function $\mathbf{1}$ (since $\mu * \mathbf{1}$ is the summatory function of μ, which is e as shown in the last exercise). Hence we obtain

$$\hat{\varphi}(n) = (\hat{\mathrm{id}} * \hat{\mu})(n) = \sum_{d|n} \mu(d)d.$$

The identity $\sum_{d|n} \mu(d)d = \prod_{p|n}(1-p)$ follows from the first exercise, with $f = \mathrm{id}$.

Problem 6 (Homework)**.** Show that the Dirichlet-inverse $\hat{\sigma}_k(n)$ of the divisor sum $\sigma_k(n)$ is the multiplicative function which is given on prime powers p^m by

$$\hat{\sigma}_k(p^m) = \begin{cases} -p^k - 1, & \text{if } m = 1, \\ p^k, & \text{if } m = 2, \\ 0, & \text{if } m \geq 3. \end{cases}$$

Solution 6. By definition, we have $\sigma_k = \mathbf{1} * p_k$, where $p_k(n) = n^k$ is a strictly multiplicative function. Hence, the inverse is given by $\hat{\sigma}_k = \hat{\mathbf{1}} * \hat{p}_k$. We know that $\hat{\mathbf{1}} = \mu$, and, by the last problem, $\hat{p}_k(n) = \mu(n)p_k(n)$ since p_k is strictly multiplicative. This give the formula

$$\hat{\sigma}_k(n) = (\hat{\mathbf{1}} * \hat{p}_k)(n) = \sum_{d|n} \mu(n/d)\mu(d)d^k.$$

For $n = p^m$ we have

$$\hat{\sigma}_k(p^m) = \sum_{d|p^m} \mu(p^m/d)\mu(d)d^k = \sum_{j=0}^{m} \mu(p^{m-j})\mu(p^j)p^{jk}.$$

Hence

$$\hat{\sigma}_k(p) = \mu(p) + \mu(p)p^k = -1 - p^k,$$

and

$$\hat{\sigma}_k(p^2) = \mu(p^2) + \mu(p)\mu(p)p^k + \mu(p^2)p^{2k} = p^k.$$

Moreover, for $m > 2$, one of $m - j$ and j will be least 2 for any j, so $\mu(p^{m-j}) = 0$ or $\mu(p^j)$, so all summands in $\hat{\sigma}_k(p^m)$ vanish for $m > 2$.

Problem 7 (sage)**.** Write a function that

1. computes the Dirichlet convolution of two number-theoretic functions f, g.
2. computes the Dirichlet-inverse $\hat{f}$ of a number-theoretic function f.