# Solutions 11

## Zeta Functions

1. Consider real numbers $1 < a_1 < a_2 < \ldots$ with $\sum_{k=1}^{\infty} a_k^{-1} = \infty$. For any integer $n$ let $b_n$ denote the number of $k \geqslant 1$ with $a_k \leqslant n$. Prove that for every $\varepsilon > 0$:

   (a) There exist infinitely many $k$ with $a_k \leqslant \varepsilon k(\log k)^{1+\varepsilon}$.

   (b) There exist infinitely many $n$ with $b_n \geqslant \frac{n}{\varepsilon(\log n)^{1+\varepsilon}}$.

   *(c) Suppose that $a_k = k(\log k)^c$ for some constant $c \geqslant 0$. Determine the asymptotic behavior of $\sum a_k^{-s}$ for real $s \to 1+$.

   **Solution**: (a) If not, there exists $\varepsilon > 0$ such that $a_k \geqslant \varepsilon k(\log k)^{1+\varepsilon}$ for all $k \geqslant 2$. Then $\sum_{k=1}^{\infty} a_k^{-1} \leqslant a_1^{-1} + \frac{1}{\varepsilon}\sum_{k=2}^{\infty} \frac{1}{k(\log k)^{1+\varepsilon}}$. The latter series converges because

$$\int_2^\infty \frac{1}{x(\log(x))^{1+\varepsilon}}\, dx \overset{y=\log(x)}{=} \int_{\log 2}^\infty \frac{1}{y^{1+\varepsilon}}\, dy = -\frac{1}{\varepsilon y^\varepsilon}\bigg|_{\log 2}^\infty < \infty.$$

   Hence $\sum_{k=1}^{\infty} a_k^{-1} < \infty$, contradicting our assumption.

   (b) If not, there exists $\varepsilon > 0$ such that $b_n \leqslant \frac{n}{\varepsilon(\log n)^{1+\varepsilon}}$ for all $n$. In particular for all $k$ we have $k = b_{a_k} \leqslant \frac{a_k}{\varepsilon(\log a_k)^{1+\varepsilon}}$ and hence $\varepsilon k(\log a_k)^{1+\varepsilon} \leqslant a_k$. This implies that $\varepsilon k(\log a_1)^{1+\varepsilon} \leqslant a_k$ and hence $\varepsilon k(c+\log k)^{1+\varepsilon} \leqslant a_k$ for $c := \log(\varepsilon(\log a_1)^{1+\varepsilon})$. Thus we have $\frac{\varepsilon}{2}k(\log k)^{1+\varepsilon} \leqslant a_k$ for all $k \gg 0$, contradicting (a).

   (c) The answer is:

$$\sum a_k^{-s} \;\sim\; \begin{cases} 1 & \text{if } c > 1, \\ \log\frac{1}{s-1} & \text{if } c = 1, \\ (s-1)^{c-1} & \text{if } 0 \leqslant c < 1, \end{cases}$$

   where $\sim$ means that the ratio of the two sides is bounded away from 0 and from $\infty$.

   *Sketch of proof:* As the function $x \mapsto (x(\log x)^c)^{-s}$ is monotone decreasing, we have

$$\sum_k (k(\log k)^c)^{-s} \;=\; O(1) + \int_2^\infty (x(\log x)^c)^{-s} dx.$$

   The substitution $x = e^y$ turns this into

$$O(1) + \int_1^\infty (e^y y^c)^{-s} e^y dy \;=\; O(1) + \int_1^\infty y^{-cs} e^{-y(s-1)} dy,$$

If $c > 1$, this converges for $s \to 1+$ to

$$O(1) + \int_1^\infty y^{-c} dy \;=\; O(1) + \tfrac{1}{c-1} \;=\; O(1),$$

yielding the stated answer. If $c \leqslant 1$ we use the substitution $y(s-1) = z$ to obtain

$$O(1) + \int_{s-1}^\infty \left(\tfrac{z}{s-1}\right)^{-cs} e^{-z} \tfrac{dz}{s-1} \;=\; O(1) + (s-1)^{cs-1} \int_{s-1}^\infty z^{-cs} e^{-z} dz.$$

Here $(s-1)^{cs-1} \sim (s-1)^{c-1}$, because $(s-1)^{s-1} \to 1$ for $s \to 1+$. To estimate the last integral we break it up at $z = 1$. The integral over $[1, \infty)$ is bounded by $\int_1^\infty e^{-z} dz = e^{-1}$. By contrast, for all $z \in [0, 1]$ we have $e^{-1} \leqslant e^{-z} \leqslant 1$; hence the integral over $[s-1, 1]$ is

$$\int_{s-1}^1 z^{-cs} e^{-z} dz \;\sim\; \int_{s-1}^1 z^{-cs} dz \;=\; \left.\frac{z^{1-cs}}{1-cs}\right|_{s-1}^1 \;=\; \frac{1-(s-1)^{1-cs}}{1-cs}$$

provided that $cs \neq 1$. In the case $c < 1$ we have $cs < 1$ for all $s$ near 1, so the right hand side is $\sim 1$, yielding the stated answer. In the case $c = 1$ the result is

$$\begin{aligned}
\sim\; O(1) + \frac{1-(s-1)^{1-s}}{1-s} \;&=\; O(1) + \frac{e^{-(s-1)\log(s-1)} - 1}{s-1} \\
&=\; O(1) + \frac{-(s-1)\log(s-1) + O(((s-1)\log(s-1))^2)}{s-1} \\
&=\; O(1) + \log\frac{1}{s-1} + o(s-1) \\
&\sim\; \log\frac{1}{s-1},
\end{aligned}$$

which is again the stated answer.

2. Show that for any $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$ we have

   (a)
   $$\zeta(s)^{-1} \;=\; \sum_{n=1}^\infty \frac{\mu(n)}{n^s},$$
   where $\mu$ denotes the Möbius function.

   (b)
   $$\zeta(s)^2 \;=\; \sum_{n=1}^\infty \frac{d(n)}{n^s},$$
   where $d(n)$ is the number of divisors of $n$.

(c)

$$\frac{\zeta'(s)}{\zeta(s)} \;=\; -\sum_{p \text{ prime}} \sum_{n=1}^{\infty} \frac{\log p}{p^{ns}}.$$

*(d)

$$\log \zeta(s) \;=\; s \cdot \int_2^{\infty} \frac{\pi(x)}{x(x^s - 1)}\, dx,$$

where $\pi(x)$ denotes the number of primes $p \leqslant x$.

**Solution**:

(a) The Euler product formula (Proposition 7.1.7) states that

$$\zeta(s) = \prod_{p \text{ prime}} (1 - p^{-s})^{-1}.$$

By taking the inverse on both sides, we obtain

$$\zeta(s)^{-1} = \prod_{p \text{ prime}} (1 - p^{-s}).$$

For $N > 0$, let $2 = p_1 < \cdots < p_M$ denote the prime numbers $\leqslant N$. We have

$$\prod_{i=1}^{M} (1 - p_i^{-s}) = \sum_{k_1,\ldots,k_M \in \{0,1\}} (-1)^{\sum_{i=1}^{M} k_i} \prod_{i=1}^{M} p_i^{-sk_i} = \sum_{\substack{n \in \mathbb{Z}^{\geqslant 1} \\ \text{prime factors of } n \text{ are } \leqslant N}} \mu(n) n^{-s}.$$

The right hand side converges absolutely for $N \to \infty$ as its terms are bounded in absolute value by a reordering of the terms of $\zeta(s)$ which converges absolutely. In the limit we thus obtain the desired formula by reordering the terms of the right hand side.

(b) See e.g. `https://proofwiki.org/wiki/Square_of_Riemann_Zeta_Function` using the fact that the product of two absolutely convergent series is absolutely convergent.

(c),(d) See pages 67-69 in [K. Chandrasekharan: Lectures on the Riemann Zeta Function. Lectures on mathematics and physics. Tata Institute of Fundamental Research, Bombay, 1953].

3. Let $\mathbb{F}_q$ denote a finite field of cardinality $q$, and consider a ring of the form $A := \mathbb{F}_q[X_1, \ldots, X_r]/(f_1, \ldots, f_s)$ for polynomials $f_1, \ldots, f_s$. For every ideal $\mathfrak{a} \subset A$ of finite index set $\deg(\mathfrak{a}) := \dim_{\mathbb{F}_q}(A/\mathfrak{a})$. The *formal zeta function* of $A$ is the formal power series

$$Z(T) \;:=\; \prod_{\mathfrak{m} \subset A} (1 - T^{\deg(\mathfrak{m})})^{-1} \;\in\; \mathbb{Z}[[T]]^{\times},$$

where the product is extended over all maximal ideals $\mathfrak{m} \subset A$. For any integer $n \geqslant 1$ let $\mathbb{F}_{q^n}$ be an extension of degree $n$ and put

$$X(\mathbb{F}_{q^n}) \;:=\; \big\{\underline{x} \in (\mathbb{F}_{q^n})^r \;\big|\; f_1(\underline{x}) = \ldots = f_s(\underline{x}) = 0\big\}.$$

(*Explanation:* Here $X$ denotes the affine algebraic variety over $\mathbb{F}_q$ defined by the equations $f_1 = \ldots = f_s = 0$, and $A$ is its coordinate ring.)

(a) Prove that $Z(T)$ is well-defined and satisfies

$$T\frac{d}{dT}\log Z(T) \;=\; T\frac{Z'(T)}{Z(T)} \;=\; \sum_{n\geqslant 1} |X(\mathbb{F}_{q^n})| \cdot T^n.$$

(b) If $A$ is a Dedekind ring prove that

$$Z(T) \;=\; \sum_{0\neq\mathfrak{a}\subset A} T^{\deg(\mathfrak{a})}.$$

(c) In the case $A := \mathbb{F}_q[X_1, \ldots, X_r]$ prove that

$$Z(T) \;=\; (1 - q^r T)^{-1}.$$

(d) Prove that the number $N_d$ of monic irreducible polynomials of degree $d$ in $\mathbb{F}_q[X]$ satisfies

$$N_d \;=\; \tfrac{1}{d} \cdot \sum_{k|d} \mu(\tfrac{d}{k}) q^k,$$

where $\mu$ is the Möbius function.

**Solution**: (a) Any point $\underline{x} \in X(\mathbb{F}_{q^n})$ determines an $\mathbb{F}_q$-algebra homomorphism

$$\varphi_{\underline{x}} \colon A \longrightarrow \mathbb{F}_{q^n},\; f(\underline{X}) \mapsto f(\underline{x}),$$

and conversely any $\mathbb{F}_q$-algebra homomorphism $A \to \mathbb{F}_{q^n}$ arises in this way from a unique point in $X(\mathbb{F}_{q^n})$. Moreover, the kernel $\mathfrak{m}_{\underline{x}}$ of $\varphi_{\underline{x}}$ is a maximal ideal of $A$ and $\varphi_{\underline{x}}$ corresponds to an embedding $A/\mathfrak{m}_{\underline{x}} \hookrightarrow \mathbb{F}_{q^n}$. Thus the residue field $A/\mathfrak{m}_{\underline{x}}$ is an extension of $\mathbb{F}_q$ of degree dividing $n$.

Conversely, for any maximal ideal $\mathfrak{m} \subset A$ the residue field $A/\mathfrak{m}$ is a field extension of $\mathbb{F}_q$ that is finitely generated as an $\mathbb{F}_q$-algebra. It is therefore a finite extension of $\mathbb{F}_q$ of degree $\deg(\mathfrak{m}) < \infty$. By Galois theory, there exists an embedding $A/\mathfrak{m} \hookrightarrow \mathbb{F}_{q^n}$ if and only if $\deg(\mathfrak{m})|n$, and the number of embeddings is then $\deg(\mathfrak{m})$. Together this shows that

$$(*) \qquad |X(\mathbb{F}_{q^n})| \;=\; \sum_{\substack{\mathfrak{m}\subset A \\ \deg(\mathfrak{m})|n}} \deg(\mathfrak{m}).$$

Note that $X(\mathbb{F}_{q^n})$ is a finite set, because there are only finitely many possibilities for the coefficients of $\underline{x}$. Thus $(*)$ implies that for every integer $d \geqslant 1$ there exist at most finitely many maximal ideals $\mathfrak{m}$ with $\deg(\mathfrak{m}) = d$. This shows that the product defining $Z(T)$ converges in $\mathbb{Z}[[T]]^\times$; hence $Z(T)$ is well-defined.

Now we can calculate

$$\begin{aligned}
T\frac{d}{dT}\log Z(T) &= -T\frac{d}{dT}\sum_{\mathfrak{m}\subset A}\log(1-T^{\deg(\mathfrak{m})}) \\
&= -T\sum_{\mathfrak{m}\subset A}\frac{-\deg(\mathfrak{m})T^{\deg(\mathfrak{m})-1}}{1-T^{\deg(\mathfrak{m})}} \\
&= \sum_{\mathfrak{m}\subset A}\deg(\mathfrak{m})\sum_{k=1}^{\infty}T^{k\deg(\mathfrak{m})} \\
&= \sum_{n=1}^{\infty}\sum_{\substack{\mathfrak{m}\subset A\\ \deg(\mathfrak{m})|n}}\deg(\mathfrak{m})T^n \\
&= \sum_{n=1}^{\infty}|X(\mathbb{F}_{q^n})|\cdot T^n.
\end{aligned}$$

(b) This follows from unique factorization of ideals in the same way as one proves the Euler product of the Riemann or Dedekind zeta function.

(c) In the case $A = \mathbb{F}_q[X_1,\ldots,X_r]$ there are no equations to satisfy; hence we have $|X(\mathbb{F}_{q^n})| = q^{rn}$. By (a) we therefore get

$$T\frac{d}{dT}\log Z(T) = \sum_{n\geqslant 1}q^{rn}T^n = \frac{q^rT}{1-q^rT} = T\frac{d}{dT}\log\frac{1}{1-q^rT}.$$

Integrating formally this shows that $Z(T)$ and $(1-q^rT)^{-1}$ differ only by a constant factor. Since both have constant coefficient 1, this factor must be 1. (*Aliter:* In the case $r = 1$ one can use (b) instead of (a).)

(d) Setting $A := \mathbb{F}_q[X]$, the number $N_d$ is the number of maximal ideals $\mathfrak{m} \subset A$ of degree $\deg(\mathfrak{m}) = d$. Thus by the formula $(*)$ we have

$$q^n = \sum_{d|n} dN_d.$$

By Möbius inversion, as in exercise 1 (b) of sheet 5, this is equivalent to

$$dN_d = \sum_{k|d}\mu(\tfrac{d}{k})q^k.$$