18.785 Number Theory **Fall 2015**
Problem Set #8 **Due: 11/16/2015**

Description

These problems are related to the material covered in Lectures 14-15. Your solutions are to be written up in latex (you can use the latex source for the problem set as a template) and submitted as a pdf-file with a filename of the form `SurnamePset8.pdf` via e-mail to `drew@math.mit.edu` by **5pm** on the date due. Collaboration is permitted/encouraged, but you must identify your collaborators, and any references you consulted. If there are none, write "**Sources consulted: none**" at the top of your problem set. The first person to spot each non-trivial typo/error in any of the problem sets or lecture notes will receive 1-5 points of extra credit.

Note: Problem 1 assumes some background in complex analysis beyond the quick review given in the notes.

Instructions: First do the warm up problems, then pick two of problems 1-4 to solve and write up your answers in latex. Finally, complete the survey problem 5.

Problem 0.

These are warm up problems that do not need to be turned in.

(a) In class we gave an elementary proof that $\vartheta(x) = O(x)$. Give a similarly elementary proof that $x = O(\vartheta(x))$ (both bounds were proved by Chebyshev before the PNT).

(b) Prove the Möbius inversion formula, which states that if f and g are functions $\mathbb{Z}_{\geq 1} \to \mathbb{C}$ that satisfy $g(n) = \sum_{d|n} f(d)$ then $f(n) = \sum_{d|n} \mu(d) g(n/d)$, where $\mu(n) := (-1)^{\#\{p|n\}}$ if n is squarefree and $\mu(n) = 0$ otherwise.

Problem 1. The explicit formula (50 points)

Let $Z(s) := \pi^{-s/2}\Gamma(\frac{s}{2})\zeta(s)$ denote the completed zeta function; we proved in class that it has the integral representation

$$Z(s) = \int_1^\infty \sum_{n=1}^\infty e^{-\pi n^2 x}(x^{s/2} + x^{(1-s)/2})\frac{dx}{x} - \frac{1}{s} - \frac{1}{1-s},$$

and extends to a meromorphic function on $\mathbb{C}$ with functional equation $Z(s) = Z(1-s)$.

Recall Hadamard's Factorization Theorem: if $f(s)$ is an entire function and n is an integer for which there exists a positive $c < n+1$ such that $|f(s)| = O\big(\exp(|s|^c)\big)$ then

$$f(s) = s^m e^{g(s)} \prod_\rho \left(1 - \frac{s}{\rho}\right) E_n\left(\frac{s}{\rho}\right), \qquad (1)$$

where $m = \operatorname{ord}_0(f)$, $g \in \mathbb{C}[s]$ has degree at most n, the product ranges overs zeros $\rho \neq 0$ of $f(s)$ (with multiplicity), and $E_n(z) = \exp(\sum_{k=1}^n \frac{z^k}{k})$.

(a) Prove that we can apply (1) to $f(s) := s(s-1)Z(s)$ with $n = 1$ and $m = 0$.

(b) Prove that we can apply (1) to $f(s) := \Gamma(s)^{-1}$ with $n = 1$ and $m = 1$.

(c) Prove that

$$(s-1)\zeta(s) = e^{a+bs} \prod_{\rho} \left(1 - \frac{s}{\rho}\right) e^{\frac{s}{\rho}} \prod_{n=1}^{\infty} \left(1 + \frac{s}{2n}\right) e^{-\frac{s}{2n}}$$

for some $a, b \in \mathbb{C}$, where ρ ranges over the zeros of $\zeta(s)$ in the critical strip.

(d) Using (c) and the Euler product for $\zeta(s)$, show that $b = \frac{\zeta'(0)}{\zeta(0)} - 1$ and

$$\sum_{p} \sum_{m \geq 1} p^{-ms} \log p = \frac{s}{s-1} - \frac{\zeta'(0)}{\zeta(0)} - \sum_{\rho} \left(\frac{1}{s-\rho} + \frac{1}{\rho}\right) - \sum_{n \geq 1} \left(\frac{1}{s+2n} - \frac{1}{2n}\right)$$

on $\mathrm{Re}(s) > 1$.

We now recall the identity

$$\frac{1}{2\pi i} \int_{\sigma - i\infty}^{\sigma + i\infty} \frac{x^s}{s} ds = \begin{cases} 1 & \text{if } x > 1, \\ 0 & \text{if } 0 < x < 1, \end{cases}$$

valid for any $x, \sigma > 0$, and define the *Perron integral transform*

$$f \mapsto \lim_{t \to \infty} \frac{1}{2\pi i} \int_{\sigma - it}^{\sigma + it} f(s) \cdot \frac{x^s}{s} ds.$$

We also define an alternative version of Chebyshev's function

$$\psi(x) := \sum_{p^n \leq x} \log p,$$

where the sum is over all prime powers $p^n \leq x$ (but note that we take $\log p$ not $\log p^n$).

(e) Fix $x > 1$ not a prime power. By applying the Perron integral transform to both sides of the equation in (d), and assuming that the RHS can be computed by applying Cauchy's residue formula term by term to the sums (and that the Perron integral transform converges in each case), deduce the *Explicit Formula*

$$\psi(x) = x - \sum_{\rho} \frac{x^{\rho}}{\rho} - \frac{\zeta'(0)}{\zeta(0)} + \sum_{n} \frac{x^{-2n}}{2n}.$$

(f) Fix $c \in [1/2, 1)$ and suppose that $\zeta(s)$ has no zeros in the strip $c < \mathrm{Re}(s) < 1$. Assume that the number of zeros with imaginary part at most T is bounded by $O(T \log T)$. Derive the following bounds: $\psi(x) = x + O(x^{c+\epsilon})$, $\vartheta(x) = x + O(x^{c+\epsilon})$, and $\pi(x) = \mathrm{Li}(x) + O(x^{c+\epsilon})$, for any $\epsilon > 0$ (in fact one replace ϵ with $o(1)$).

Remark. The explicit formula you obtained in (e) is a slight variation of the one given by Riemann (who also glossed over the somewhat delicate convergence issues you were told to ignore – to make this rigorous you actually need to specify the order in which the sum over ρ is computed, it does not converge absolutely). It is worth noting that even with the explicit formula in hand, Riemann was unable to prove the Prime Number Theorem because he could not (and we still cannot) prove that one can take $c < 1$ in (f).

Problem 2. The zeta function of $\mathbb{F}_q(t)$ (50 points)

Recall that for a number field K, the Dedekind zeta function $\zeta_K(s)$ is defined by

$$\zeta_K := \sum_I N(I)^{-s},$$

where I ranges over nonzero ideals of $\mathcal{O}_K$ and $N(I)$ is the absolute norm, the cardinality of the residue field $\mathcal{O}_K/\mathfrak{p}$ when I is a prime ideal $\mathfrak{p}$. The Riemann zeta function corresponds to the case $K = \mathbb{Q}$.

We now extend this definition to all global fields K by defining the absolute norm for prime ideals $\mathfrak{p}$ via $N(\mathfrak{p}) = \#\mathcal{O}_K/\mathfrak{p}$ and extending multiplicatively. In this problem you will investigate the zeta function ζ_K of the rational function field $K := \mathbb{F}_q(t)$ with ring of integers $\mathcal{O}_K = \mathbb{F}_q[t]$.

(a) Show that every $\mathcal{O}_K$-ideal has the form $I = (f)$, with $f \in \mathbb{F}_q[x]$ monic, and then $N(I) = \#(\mathcal{O}_K/f\mathcal{O}_K) = q^{\deg f}$. Then prove that $\zeta_K = \frac{1}{1-q^{1-s}}$ for $\mathrm{Re}(s) > 1$.

(b) Prove that $\zeta_K(s)$ has the Euler product

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1},$$

valid for $\mathrm{Re}(s) > 1$.

(c) Prove that $\zeta_K(s)$ extends to a meromorphic function on $\mathbb{C}$ with a simple pole at $s = 1$ and no zeros. Give the residue of the pole at $s = 1$.

(d) Define a completed zeta function $Z(s) = G(s)\zeta_K(s)$, where $G(s)$ is some suitably chosen meromorphic function, and prove that your completed zeta function satisfies the functional equation

$$Z_K(s) = Z_K(1-s).$$

(e) Let a_d denote the number of primes of $\mathcal{O}_K$ with residue field degree d, equivalently, the number of irreducible monic polynomials in $\mathbb{F}_q[x]$ of degree d. Using (b) and (c), prove that

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

Then apply Möbius inversion to obtain

$$a_n = \frac{1}{n}\sum_{d|n} \mu(d) q^{n/d}.$$

(f) Prove the Prime Number Theorem for $\mathbb{F}_q[t]$, which states that

$$a_n = \frac{q^n}{n} + O\left(\frac{1}{n} q^{n/2}\right).$$

Remark. The error term in (f) is comparable to the error term in the PNT under the Riemann hypothesis (replace q^n with x); note that the analog of the Riemann hypothesis for $\zeta_K(s)$ is (vacuously) true, by (c).

(g) Let $S(n)$ be the set of monic polynomials of degree n in $\mathbb{F}_q[t]$, and let $I(n)$ be the subset of polynomials in $S(n)$ that are irreducible. Show that $\#I(n)/\#S(n) \sim \frac{1}{n}$. Now let $R(n)$ be the subset of polynomials in $S(n)$ that have no roots in $\mathbb{F}_q$. Give an asymptotic estimate for $\#R(n)/\#S(n)$.

(h) Let $Q(n)$ denote the subset of $S(n)$ consisting of squarefree polynomials. Prove that $\lim_{n\to\infty} \#Q(n)/\#S(n) = 1/\zeta_K(2)$.

(i) For nonzero $f \in \mathcal{O}_K$ define Φ via $\Phi(f) := \#(\mathcal{O}_K/f\mathcal{O}_K)^\times$. Prove the following

1. $\Phi(f) = N(f)\prod_{p|f}(1 - N(p)^{-1})$, where p ranges over the irreducible factors of f.
2. For all $f, g \in \mathcal{O}_K$ with $(f, g) = 1$ we have $g^{\Phi(f)} \equiv 1 \bmod f$.

Problem 3. Bernoulli numbers (50 points)

For integers $n \geq 0$, the *Bernoulli polynomials* $B_n(x) \in \mathbb{Q}[x]$ are defined as the coefficients of the exponential generating function

$$E(t, x) := \frac{te^{tx}}{e^t - 1} = \sum_{n\geq 0} \frac{B_n(x)}{n!} t^n.$$

The *Bernoulli numbers* $B_n \in \mathbb{Q}$ are defined by $B_n = B_n(0)$.

(a) Prove that $B_0(x) = 1$, $B'_n(x) = nB_{n-1}(x)$, and $B_n(1) = B_n(0)$ for $n \neq 1$, and that these properties uniquely determine the Bernoulli polynomials.

(b) Prove that $B_n(x + 1) - B_n(x) = nx^{n-1}$ and

$$B_n(x + y) = \sum_{k=0}^{n} \binom{n}{k} B_k(x)y^{n-k}.$$

Use this to show that B_k can alternatively be defined by the recurrence $B_0 = 1$ and

$$B_n = -\frac{1}{n+1} \sum_{k=0}^{n-1} \binom{n+1}{k} B_k$$

for all $n > 0$, and show that $B_n = 0$ for all odd $n > 1$.

(c) Recall the hyperbolic cotangent function $\coth z := \frac{e^z+e^{-z}}{e^z-e^{-z}}$. Prove that

$$z \coth z = \sum_{n\geq 0} B_{2n} \frac{(2z)^{2n}}{(2n)!}.$$

(d) Show that $\cot z = i \coth iz$ and prove (as Euler did)

$$z \cot z = 1 - 2 \sum_{k\geq 1} \frac{z^2}{k^2\pi^2 - z^2}.$$

(e) Use (c) and (d) to prove that for all $n \geq 1$ we have

$$\zeta(2n) = (-1)^{n-1}\frac{(2\pi)^{2n}B_{2n}}{2\cdot(2n)!},$$

and then use the functional equation to prove that for all $n \geq 1$ we have

$$\zeta(-n) = -\frac{B_{n+1}}{n+1}.$$

(f) Prove (rigorously!) that for any integer $n > 1$ the asymptotic density of integers that are *n-power free* (not divisible by p^n for any prime p) is $1/\zeta(n)$ and compute this density explicitly for $n = 2, 4, 6$.

(g) Prove that for all integer $n, N > 1$ we have

$$\sum_{m=0}^{N-1}(m+x)^{n-1} = \frac{B_n(N+x) - B_n(x)}{n}.$$

Use this to deduce Faulhaber's formula

$$P_n(N) := \sum_{m=1}^{N-1} m^n = \frac{1}{n+1}\sum_{k=0}^{n}\binom{n+1}{k}B_k N^{n+1-k}$$

for summing nth powers. Compute the polynomials $P_n(N)$ explicitly for $n = 2, 3, 4$

Problem 4. Arithmetic functions and Dirichlet series (50 points)

Recall that an *arithmetic function* is a function $a\colon \mathbb{Z}_{\geq 1} \to \mathbb{C}$; we say that $a \neq 0$ is *multiplicative* if $a(mn) = a(m)a(n)$ holds for all relatively prime m, n, and *totally multiplicative* if this holds for all m, n. Below are some examples; as usual, p denotes a prime, p^e denotes a (nontrivial) prime power, and $d|n$ indicates that d is a positive divisor of n.

- $0(n) = 0,\ \ 1(n) = 1,\ \ \mathrm{id}(n) := n,\quad e(n) := 0^{n-1};$
- $\tau(n) := \#\{d|n\},\quad \sigma(n) := \sum_{d|n} d;$
- $\omega(n) := \#\{p|n\},\ \ \Omega(n) := \#\{p^e|n\},\ \ \phi(n) := \#(\mathbb{Z}/n\mathbb{Z})^\times;$
- $\lambda(n) := (-1)^{\Omega(n)},\ \ \mu(n) := (-1)^{\omega(n)}\cdot 0^{\Omega(n)-\omega(n)},\quad \mu^2(n) := \mu(n)^2.$

The set of all arithmetic functions forms a $\mathbb{C}$-vector space that we denote $\mathcal{A}$. Associated to each arithmetic function is a *Dirichlet series* $\sum_{n\geq 1} c_n n^{-s}$ defined by

$$D_a(s) := \sum_{n\geq 1} a(n)n^{-s}$$

The *Dirichlet convolution* $a * b$ of arithmetic functions a and b is defined by

$$(a*b)(n) := \sum_{d|n} a(d)b(n/d),$$

We use f^{*n} to denote the n-fold convolution $f * \cdots * f$.

(a) Prove that for any arithmetic functions we have $D_{a*b} = D_a D_b$ and that endowing $\mathcal{A}$ with a multiplication defined by Dirichlet convolution makes $\mathcal{A}$ a $\mathbb{C}$-algebra that is isomorphic to the $\mathbb{C}$-algebra of Dirichlet series (with the usual multiplication).

(b) Show that $\mathcal{A}$ is a local ring with unit group $\mathcal{A}^\times = \{f \in \mathcal{A} : f(1) \neq 0\}$ and maximal ideal $\mathcal{A}_0 = \{f \in \mathcal{A} : f(1) = 0\}$. Prove that the set of multiplicative functions $\mathcal{M}$ forms a subgroup of $A_1 := \{f \in \mathcal{A} : f(1) = 1\} \subseteq \mathcal{A}^\times$. Is this also true of the set of totally multiplicative functions?

(c) Prove the following identities $\mu * 1 = e$, $\phi * 1 = \mathrm{id}$, $\mu * \mathrm{id} = \phi$, $1 * 1 = \tau$, $\mathrm{id} * 1 = \sigma$. Use $\mu * 1 = e$ to give a one-line proof of the Möbius inversion formula.

(d) Define the exponential map $\exp\colon \mathcal{A} \to \mathcal{A}$ by

$$\exp(f) := \sum_{n=0}^{\infty} \frac{f^{*n}}{n!} = e + f + \frac{f * f}{2} + \cdots$$

Prove that exp defines a group isomorphism from $(\mathcal{A}_0, +)$ to $(\mathcal{A}_1, *)$ with inverse

$$\log(f) := \sum_{n=1}^{\infty} \frac{(-1)^{n-1}(f - e)^{*n}}{n},$$

(e) Define $\kappa(n)$ to be $1/k$ if $n = p^k$ is a prime power and 0 otherwise. Prove that $\exp \kappa = 1$, and deduce that $\exp(-\kappa) = \mu$ and $\exp(2\kappa) = \tau$.

(f) Prove that each $f \in \mathcal{A}_1$ has a unique square-root $g \in \mathcal{A}_1$ for which $g^{*2} = f$ that we denote $f^{*1/2}$. Prove that $1^{*1/2} = \exp(\kappa/2)$ and compute $\exp(\kappa/2)(n)$ for n up to 10.

Problem 5. Survey

Complete the following survey by rating each problem you attempted on a scale of 1 to 10 according to how interesting you found it (1 = "mind-numbing," 10 = "mind-blowing"), and how difficult you found it (1 = "trivial," 10 = "brutal"). Also estimate the amount of time you spent on each problem to the nearest half hour.

	Interest	Difficulty	Time Spent
Problem 1			
Problem 2			
Problem 3			
Problem 4			

Please rate each of the following lectures that you attended, according to the quality of the material (1="useless", 10="fascinating"), the quality of the presentation (1="epic fail", 10="perfection"), the pace (1="way too slow", 10="way too fast", 5="just right") and the novelty of the material to you (1="old hat", 10="all new").

Date	Lecture Topic	Material	Presentation	Pace	Novelty
11/3	Riemann zeta function, PNT I				
11/5	PNT II, the functional equation				

Please feel free to record any additional comments you have on the problem sets and the lectures, in particular, ways in which they might be improved.