

Problem Set #9

Description

These problems are related to the material covered in Lectures 17-19. 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 via e-mail to the instructor on the due date. 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.

Instructions: First do the warm up problems, then pick two of problems 1-5 to solve and write up your answers in latex, then complete the survey problem 6.

Problem 0.

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

- (a) Show $\pi(x) := \sum_{p \leq x} 1 = \int_2^\infty (1/\log t) d\vartheta(t)$ and $\vartheta(x) := \sum_{p \leq x} \log p = \int_2^\infty \log t d\pi(t)$, and use these identities to prove

$$\vartheta(x) = \pi(x) \log x - \int_2^x \frac{\pi(t)}{t} dt, \quad \pi(x) = \frac{\vartheta(x)}{\log x} + \int_2^x \frac{\vartheta(t)}{\log^2 t} dt,$$

which provides an alternative proof that $\pi(x) \sim x/\log x$ if and only if $\vartheta(x) \sim x$.

- (b) Let χ be a primitive Dirichlet character of conductor $m > 1$. Verify the identity

$$\sum_{n \geq 1} \chi(n)x^n = \frac{1}{1-x^m} \sum_{n=1}^{m-1} \chi(n)x^n$$

and use this to prove that $\Gamma(s)L(s, \chi)$ extends to a holomorphic function on \mathbb{C} . Conclude that $L(s, \chi)$ has an analytic continuation to \mathbb{C} .

Problem 1. Mertens' Theorems (50 points)

In his 1874 paper Mertens' proved three asymptotic bounds on sums over primes; he necessarily did not rely on the Prime Number Theorem, which was proved in 1896.

Define the constants

$$\alpha := - \sum_{n \geq 2} \frac{\mu(n)}{n} \log \zeta(n) \approx 0.315718, \quad \gamma := \lim_{x \rightarrow \infty} \left(\sum_{1 \leq n \leq x} \frac{1}{n} - \log x \right) \approx 0.577216,$$

where $\mu(n)$ is the Möbius function, and let $\Lambda(n)$ denote the von Mangoldt function: $\Lambda(n) = \log p$ when $n = p^e$ is a prime power ($e \geq 1$) and $\Lambda(n) = 0$ otherwise.

Theorem (Mertens). As $x \rightarrow \infty$ we have the following asymptotic bounds:

- (1) $\sum_{p \leq x} \frac{\log p}{p} = \log x + O(1)$;
- (2) $\sum_{p \leq x} \frac{1}{p} = \log \log x + \gamma - \alpha + O\left(\frac{1}{\log x}\right)$;
- (3) $\sum_{p \leq x} \log\left(1 - \frac{1}{p}\right) = -\log \log x - \gamma + O\left(\frac{1}{\log x}\right)$.

Remark. Mertens showed that the $O(1)$ term in (1) has absolute value bounded by 2, but we won't need this. One often sees (3) written as $\prod_{p \leq x} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma + o(1)}}{\log x}$ but our version is a slightly sharper statement and reflects what Mertens actually proved.

(a) Show that $\log(n) = \sum_{d|n} \Lambda(d)$ and derive the bounds

$$\sum_{n \leq x} \log n = \sum_{d \leq x} \Lambda(d) \left\lfloor \frac{x}{d} \right\rfloor \quad \text{and} \quad \sum_{d \leq x} \frac{\Lambda(d)}{d} = \log x + O(1).$$

Use these bounds and Stirling's formula to prove (1).

(b) Let $A(x)$ denote the sum in (1). Prove that

$$\sum_{p \leq x} \frac{1}{p} = \frac{A(x)}{\log x} + \int_2^x \frac{A(t)}{t(\log t)^2} dt = \log \log x + c + O\left(\frac{1}{\log x}\right),$$

for some constant c .

(c) Prove that for $\operatorname{Re}(s) > 1$ we have

$$\frac{1}{s} \log \zeta(s) = \int_2^\infty \frac{\pi(t) dt}{t(t^s - 1)},$$

and for $t > 1$ we have

$$\frac{1}{t^2(t-1)} = -\sum_{n \geq 2} \frac{\mu(n)}{t(t^n - 1)}.$$

(d) Prove that

$$\sum_{n \geq 2} \sum_p \frac{1}{np^n} = \int_2^\infty \frac{\pi(t) dt}{t^2(t-1)} = \alpha$$

and deduce that (2) and (3) are equivalent.

Remark. Parts (b) and (d) imply that (3) holds if we replace γ with $c' = c + \alpha$. Problem 2 gives a proof that in fact $c' = \gamma$, so both (2) and (3) hold.

(e) Let $P(x) := \sum_{p \leq x} \frac{1}{p} = \log \log x + c + \epsilon(x)$ with $\epsilon(x) = O\left(\frac{1}{\log x}\right)$ as in (b). Show that

$$\pi(x) = \int_{2^-}^x t dP(t) = O\left(\frac{x}{\log x}\right),$$

and that with the error bound $\epsilon(x) = o\left(\frac{1}{\log x}\right)$ one obtains $\pi(x) \sim \frac{x}{\log x}$. Thus a slightly stronger version of Mertens' 2nd theorem implies the prime number theorem.

Problem 2. Mellin transforms of Dirichlet series (50 points)

Recall that an *arithmetic function* is a function $f: \mathbb{Z}_{n \geq 1} \rightarrow \mathbb{C}$, and it defines a Dirichlet series

$$D_f(s) := \sum_{n \geq 1} f(n)n^{-s},$$

which we may view a function of the complex variable s on any region $\operatorname{Re}(s) > \sigma \geq 0$ in which the series converges. Associated to any arithmetic function f is the *summatory function* $S_f: \mathbb{R} \rightarrow \mathbb{C}$ defined by

$$S_f(x) := \sum_{1 \leq n \leq x} f(n),$$

and the *logarithmic summatory function* $L_f: \mathbb{R} \rightarrow \mathbb{C}$ defined by

$$L_f(x) := \sum_{1 \leq n \leq x} \frac{f(n)}{n}.$$

(a) Show that $D_f(s)$ is related to $S_f(x)$ and $L_f(x)$ via the formulas

$$\begin{aligned} D_f(s) &= s \int_1^\infty S_f(t)t^{-s-1} dt && (\operatorname{Re}(s) > \max(0, \sigma)), \\ D_f(s) &= (s-1) \int_1^\infty L_f(t)t^{-s} dt && (\operatorname{Re}(s) > \max(1, \sigma)). \end{aligned}$$

(b) By Applying (a) to $f = 1$, show that

$$\zeta(s) = \frac{s}{s-1} - s \int_1^\infty \{t\}t^{-s-1} dt \quad (\operatorname{Re}(s) > 0),$$

where $\{t\} := t - \lfloor t \rfloor$. Use this to show that as $s \rightarrow 1$ we have

$$\zeta(s) = \frac{1}{s-1} + \gamma + O(|s-1|).$$

(c) Let

$$P(x) := - \sum_{p \leq x} \log\left(1 - \frac{1}{p}\right)$$

be the negation of the sum in Mertens' 3rd theorem (see Problem 1), and let $\kappa(n)$ be the arithmetic function defined by $\kappa(n) = 1/k$ when $n = p^k$ is a prime power ($k \geq 1$) and $\kappa(n) = 0$ otherwise (as in Problem 4.e on Problem set 8). Show that

$$P(x) = L_\kappa(x) + O\left(\frac{1}{\log x}\right).$$

(d) Show that $\log \zeta(s) = D_\kappa(s)$ and use (b) to prove that

$$D_\kappa(s) = \log \frac{1}{s-1} + O(s-1)$$

as $s \rightarrow 1^+$ (along the real line).

From parts (b) and (d) of Problem 1 we know that

$$P(x) = \log \log x + C + O\left(\frac{1}{\log x}\right) \quad (1)$$

for some constant C which, according to Mertens' 3rd theorem, is equal to Euler's constant γ . You are now in a position to prove this.

(e) From (c) and (1) we know that $L_\kappa = \log \log x + C + O\left(\frac{1}{\log x}\right)$. By plugging this into to the formula relating D_κ and L_κ from (a), show that we have

$$D_\kappa(s) = \log \frac{1}{s-1} + C + \int_0^\infty (\log t)e^{-t} dt + O\left((s-1) \log \frac{1}{s-1}\right)$$

as $s \rightarrow 1^+$.

(f) By combining (d) and (e) and letting $s \rightarrow 1^+$ show that

$$C = - \int_0^\infty (\log t)e^{-t} dt.$$

Then show that the integral is equal to $\Gamma'(1)$, and prove that $\Gamma'(1) = -\gamma$ (you can do this either by using (b) and the functional equation for $\zeta(s)$, or by evaluating the *digamma function* $\Psi(s) := \Gamma'(s)/\Gamma(s)$ at 1).

Problem 3. Dirichlet density (50 points)

Let K be a global field and let \mathcal{P} be the set of nonzero prime ideals of \mathcal{O}_K . The *natural density* of a set $S \subseteq \mathcal{P}$ is defined by

$$\delta(S) := \lim_{x \rightarrow \infty} \frac{\#\{\mathfrak{p} \in S : N(\mathfrak{p}) \leq x\}}{\#\{\mathfrak{p} \in \mathcal{P} : N(\mathfrak{p}) \leq x\}}$$

(whenever this limit exists), and its *Dirichlet density* is defined by

$$d(S) := \lim_{s \rightarrow 1^+} \frac{\sum_{\mathfrak{p} \in S} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p} \in \mathcal{P}} N(\mathfrak{p})^{-s}}$$

(whenever this limit exists). Here $N(\mathfrak{p}) := [\mathcal{O}_K : \mathfrak{p}]$ is the absolute norm.

(a) Show that the denominator in $d(S)$ is finite for real $s > 1$ and that

$$\sum_{\mathfrak{p} \in \mathcal{P}} N(\mathfrak{p})^{-s} \sim \log\left(\frac{1}{s-1}\right)$$

as $s \rightarrow 1^+$.

(b) Let S and T be subsets of \mathcal{P} with Dirichlet densities. Show that $S \subseteq T$ implies $d(S) \leq d(T)$, and that $d(S) = 0$ when S is finite. Conclude that if S and T differ by a finite set (that is, the sets $S - T$ and $T - S$ are both finite), then $d(S) = d(T)$.

(c) Suppose $S, T \subset \mathcal{P}$ have finite intersection. Show that if any two of the set S , T , and $S \cup T$ have a Dirichlet density then so does the third and $d(S \cup T) = d(S) + d(T)$.

- (d) Suppose K is a number field or a finite separable extension of $\mathbb{F}_p(t)$ and define $\mathcal{P}_1 := \{\mathfrak{p} \in \mathcal{P} : N(\mathfrak{p}) \text{ is prime}\}$. Show that $d(\mathcal{P}_1) = 1$ and therefore \mathcal{P}_1 is infinite.
- (e) With K and \mathcal{P}_1 as in (c) show for any $S \subseteq \mathcal{P}$, if S has a Dirichlet density then $d(S) = d(S \cap \mathcal{P}_1)$ and otherwise $S \cap \mathcal{P}_1$ does not have a Dirichlet density. Compute the density of the set of primes of $\mathbb{Q}(i)$ that lie above a prime $p \equiv 3 \pmod{4}$.
- (f) Show that if $S \subseteq \mathcal{P}$ has a natural density then it has Dirichlet density $d(S) = \delta(S)$.
- (g) Show that for $K = \mathbb{F}_q(t)$ the set of primes (f) where f is an irreducible polynomial of even degree has Dirichlet density $1/2$ but no natural density.
- (h) Show that for $K = \mathbb{Q}$ the set S_1 of primes whose leading decimal digit is equal to 1 has no natural density.
- (i) Let A be the set of positive integers with leading decimal digit equal to 1. Show that

$$\lim_{s \rightarrow 1^+} \frac{\sum_{n \in A} n^{-s}}{\frac{1}{s-1}} = \lim_{s \rightarrow 1^+} \frac{\sum_{n \in A} n^{-s}}{\sum_{n \geq 1} n^{-s}} = \log_{10}(2).$$

- (j) Adapt your argument in (i) to show that $d(S_1) = \log_{10}(2)$.

Problem 4. PNT for arithmetic progressions (50 points)

For each integer $m > 1$ and integer a coprime to m we define the prime counting function

$$\pi(x; m, a) := \sum_{\substack{p \leq x \\ p \equiv a \pmod{m}}} 1.$$

In this problem you will adapt the proof of the PNT in [4] (which is essentially the same as given in class except for the argument to show that $\zeta(s)$ has no zeros on $\text{Re}(s) = 1$) to prove the PNT for arithmetic progressions, which states that

$$\pi(x; m, a) \sim \frac{\pi(x)}{\phi(m)} \sim \frac{1}{\phi(m)} \frac{x}{\log x},$$

where $\phi(m) := \#(\mathbb{Z}/m\mathbb{Z})^\times$ is the Euler function. We first set some notation.

Let χ denote a primitive Dirichlet character of conductor dividing m and define

$$L(s, \chi) := \sum_{n \geq 1} \chi(n) n^{-s}, \quad \theta_{m,a}(x) := \phi(m) \sum_{\substack{p \leq x \\ p \equiv a \pmod{m}}} \log p,$$

$$\phi(s, \chi) := \sum_p \chi(p) p^{-s} \log p, \quad \Phi_m(s) := \sum_\chi \phi(s, \chi), \quad \Phi_{m,a}(s) := \sum_\chi \overline{\chi(a)} \phi(s, \chi).$$

Finally, let $K = \mathbb{Q}(\zeta_m)$ be the m th cyclotomic field with Dedekind zeta function $\zeta_K(s)$.

- (a) Show that $\theta_{m,a}(x) = O(x)$.

(b) Show that for each χ we have

$$-\frac{L'(s, \chi)}{L(s, \chi)} = \phi(s, \chi) + h(s, \chi),$$

for some $h(s, \chi)$ holomorphic on $\operatorname{Re}(s) > 1/2$, and conclude that

$$-\frac{\zeta'_K(s)}{\zeta_K(s)} = \Phi_m(s) + h(s),$$

for some $h(s)$ holomorphic on $\operatorname{Re}(s) > 1/2$.

(c) Show that $\zeta_K(s)$ is real-valued on real values of s and proceed as in step (IV) of [4] to show that $\zeta_K(s)$, and therefore each $L(s, \chi)$, has no zeros on $\operatorname{Re}(s) = 1$.

(d) Show that $\Phi_{m,a}(s) - \frac{1}{s-1}$ is holomorphic on $\operatorname{Re}(s) \geq 1$ and prove that

$$\Phi_{m,a}(s) = s \int_0^\infty e^{-st} \theta_{m,a}(e^t) dt$$

(e) Show that the Laplace transform of $f(t) = \theta_{m,a}(e^t)e^{-t} - 1$ extends to a holomorphic function on $\operatorname{Re}(s) \geq 0$ and use this to prove $\theta_{m,a}(x) \sim x$.

(f) Show that (e) implies

$$\pi(x, m) \sim \frac{\pi(x)}{\phi(m)} \sim \frac{1}{\phi(m)} \frac{x}{\log x}.$$

Problem 5. Factoring with the analytic class number formula (50 points)

Let K be an imaginary quadratic field with discriminant $D < 0$. Recall from Problem 2 of Problem Set 7 that each ideal class in $\operatorname{cl} \mathcal{O}_K$ can be uniquely represented by a reduced binary quadratic form

$$f(x, y) = ax^2 + bxy + cy^2$$

which we compactly denote $f = (a, b, c)$. The coefficients a, b, c are integers with no common factor with $a > 0$ and $b^2 - 4ac = D$ (so f is integral, primitive, positive definite, and of discriminant D), and if

$$-a < b \leq a < c \quad \text{or} \quad 0 \leq b \leq a = c,$$

then we say that f is *reduced*, and in this case $a \leq \sqrt{|D|/3}$. Every form is *equivalent* (under the action of $\operatorname{SL}_2(\mathbb{Z})$) to a unique reduced form (a, b, c) that corresponds to an ideal $I(f) = a\mathbb{Z} + a\tau\mathbb{Z}$ of norm a in the class it represents, where

$$\tau := \frac{-b + \sqrt{D}}{2a}$$

and $\mathcal{O}_K = \mathbb{Z} + a\tau\mathbb{Z}$. Let σ be the non-trivial element of $\operatorname{Gal}(K/\mathbb{Q})$. If \mathfrak{a} is an ideal, then $\bar{\mathfrak{a}} := \sigma(\mathfrak{a})$ denotes its Galois conjugate.

Everything above also applies to orders $\mathcal{O} \subseteq \mathcal{O}_K$ that are not necessarily maximal, provided we restrict our attention to ideals whose norms are prime to the conductor $c := [\mathcal{O}_K : \mathcal{O}]$. We now work in this greater generality and consider binary quadratic forms of discriminant $D = c^2 \operatorname{disc} \mathcal{O}_K$ and the class group $\operatorname{cl} \mathcal{O}$ (the group of ideals prime to the conductor modulo equivalence of principal ideals).

- (a) Show that the identity element in $\text{cl } \mathcal{O}$ is represented by the form $(1, 0, -D/4)$ when D is even and $(1, 1, (1 - D)/4)$ when D is odd.
- (b) Let \mathfrak{a} be an ideal with Galois conjugate $\bar{\mathfrak{a}}$ then $\mathfrak{a}\bar{\mathfrak{a}} = (N(\mathfrak{a}))$ and therefore $[\mathfrak{a}]^{-1} = [\bar{\mathfrak{a}}]$. Show that in terms of forms, if $\mathfrak{a} = I(f)$ with $f = (a, b, c)$ then $\bar{\mathfrak{a}}$ corresponds to the form $(a, -b, c)$, and if $(a, -b, c)$ is not reduced then we must have $b = a$ or $a = c$, but in both these cases $(a, -b, c)$ is equivalent to (a, b, c) .
- (c) An *ambiguous form* $f = (a, b, c)$ is a reduced form for which one of the following holds: $b = 0$, $b = a$, or $c = a$. Show that every ambiguous form corresponds to an ideal class that is equal to its inverse (hence has order 1 or 2), and conversely.
- (d) Show that if D is odd then the ambiguous forms of discriminant D are those of the form

$$\left(\frac{u+v}{4}, \frac{v-u}{2}, \frac{u+v}{4}\right)$$

with $uv = -D$, $\gcd(u, v) = 1$, and $0 < v/3 \leq u \leq v$, and those of the form

$$\left(u, u, \frac{u+v}{4}\right)$$

with $uv = -D$, $\gcd(u, v) = 1$, and $0 < u \leq v/3$.

- (e) Show that if D is odd and has k distinct prime factors then there are 2^{k-1} ambiguous forms, each representing a 2-torsion element of $\text{cl } \mathcal{O}$ (an ideal class of order 1 or 2), and conversely, that every 2-torsion element of $\text{cl } \mathcal{O}$ is represented by an ambiguous form. Conclude that the 2-torsion subgroup of $\text{cl } \mathcal{O}$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{k-1}$ and that every ideal class of order 1 or 2 is represented by an ambiguous form.
- (f) Let $n > 1$ be an integer coprime to 6, not a perfect power. Show that if $n \equiv 3 \pmod{4}$ then for the discriminant $D = -n$ every ideal class in $\text{cl } \mathcal{O}$ of order 2 (of which there is at least one) is represented by an ambiguous form whose coefficients yield a nontrivial factorization uv of n ; show that if $n \equiv 1 \pmod{4}$ then for the discriminant $D = -3n$ a similar statement holds for all but one ideal class of order 2 (of which there are at least 3).
- (g) Show that for $\mathcal{O} = \mathcal{O}_K$ we have $\#\text{cl } \mathcal{O} = \frac{1}{\pi} \sqrt{|D|} L(1, \chi)$, where χ is the Dirichlet character defined by the Kronecker symbol $\left(\frac{D}{\cdot}\right)$ (so $\chi(n) = \left(\frac{D}{n}\right)$). This also holds for $\mathcal{O} \subsetneq \mathcal{O}_K$, but you are not required to prove this.

The Extended Riemann Hypothesis (ERH) states that the zeros of every Dirichlet L -function $L(s, \chi)$ all lie on the critical line $\text{Re}(s) = \frac{1}{2}$. Under this assumption there is an effectively computable constant c_1 such that if we compute the partial product

$$L^* := \prod_{p \leq n^{1/5}} (1 - \chi(p)p^{-1})^{-1}$$

of $L(1, \chi)$ and put $h^* := \frac{1}{\pi} \sqrt{|D|} L^*$ (with $D < -4$), then for $h = \#\text{cl } \mathcal{O}$ we have

$$|h - h^*| < c_1 n^{2/5} (\log n)^2;$$

as shown in [3]. The ERH also implies the existence of an effectively computable constant c_2 for which the set of ideals of prime norm $a \leq c_2 \log^2 |D|$ are enough to generate $\text{cl } \mathcal{O}$; this follows from results in [2] (for $\mathcal{O} = \mathcal{O}_K$ one can take $c_2 = 6$, see [1]).

- (h) Describe a deterministic $O(n^{1/5+o(1)})$ algorithm that, given an integer $n > 1$ does one of the following: (1) outputs a nontrivial factorization of n , (2) proves that n is prime, (3) proves that the ERH is false. Assume arithmetic operations on integers (and rational numbers) can be performed in quasi-linear time (i.e. $O(b^{1+o(1)})$ where b is the number of bits in the operands). You do not need to spell out all the details of the algorithm, a summary of each step is sufficient (note: you will need to address the case where n is a perfect power separately).

Problem 6. 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			
Problem 5			

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
11/15	Analytic class number formula				
11/17	Kronecker-Weber theorem				

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.

References

- [1] E. Bach, *Explicit bounds for primality testing and related problems*, Math. Comp. **55** (1990), 335–380.
- [2] J.C. Lagarias, H.L. Montgomery, and A.M. Odlyzko, *A bound for the least prime ideal in the Chebotarev Density Theorem*, Invent. Math. **54** (1979), 271–296.
- [3] R. Schoof, *Quadratic fields and factorization*, in “Computational Methods in Number Theory”, MC-Tracts 154/155, 1982, 235–286.
- [4] D. Zagier, *Newman’s short proof of the prime number theorem*, Amer. Math. Monthly **104** (1997), 705–708.

MIT OpenCourseWare
<https://ocw.mit.edu>

18.785 Number Theory I
Fall 2016

For information about citing these materials or our Terms of Use, visit: <https://ocw.mit.edu/terms>.