C3.8 Analytic Number Theory: Sheet #1

Due on October 15, 2025 at 12:00pm

Professor B. Green

Ray Tsai

Problem 1

Prove the following.

(i) $(\log X)^4 < X^{1/10}$ for all sufficiently large X.

Proof. By L'Hopital's rule,

$$\lim_{X\to\infty} \frac{X}{e^{X^{1/40}}} = \lim_{X\to\infty} \frac{40}{X^{-39/40}e^{X^{1/40}}} = 0.$$

Thus, $X < e^{X^{1/40}}$ for all sufficiently large X. The result now follows from taking logarithms on both sides. □

(ii) $e^{\sqrt{\log X}} = O_\varepsilon(X^\varepsilon)$ for all $\varepsilon > 0$ and $X \geq 1$.

Proof. Fix $\varepsilon > 0$. Since

$$\lim_{X\to\infty} \frac{X^\varepsilon}{e^{\sqrt{\log X}}} = \lim_{X\to\infty} \frac{e^{\varepsilon \log X}}{e^{\sqrt{\log X}}} = \lim_{Y\to\infty} e^{Y(\varepsilon Y - 1)}.$$

Since $Y(\varepsilon Y - 1) \to \infty$ as $Y \to \infty$, the result now follows. □

(iii) $X(1 + e^{-\sqrt{\log X}}) + X^{3/4}\sin X \sim X$.

Proof. First note that $|X^{3/4}\sin X| \leq X^{3/4} = o(X)$, and $e^{-\sqrt{\log X}} = o(1)$. Hence, $X(1 + e^{-\sqrt{\log X}}) + X^{3/4}\sin X = (1 + o(1))X$. □

Problem 2

In the following exercise, $a(X)$, $b(X)$ are positive functions tending to ∞ as $X \to \infty$. Say whether each of the following is true or false.

(i) If $a(X) - b(X) \to 0$ then $a(X) \sim b(X)$.

Proof. True, as
$$\left|\frac{a(X)}{b(X)} - 1\right| = \left|\frac{a(X) - b(X)}{b(X)}\right| \to 0.$$
$\square$

(ii) If $a(X) \sim b(X)$ then $a(X) - b(X) \to 0$.

Proof. False. Consider $a(X) = X^2 + X$ and $b(X) = X^2$. Then $a(X) \sim b(X)$ but $a(X) - b(X) \to \infty$. $\square$

(iii) If $a(X) \sim b(X)$ and $a'(X) := \sum_{y \le X} a(y)$, $b'(X) := \sum_{y \le X} b(y)$ then $a'(X) \sim b'(X)$.

Proof. True. Fix $\varepsilon > 0$. By definition, there exists $X_0 = X_0(\varepsilon)$ such that $a(y) \ge (1-\varepsilon)b(y)$ for $y \ge X_0$. But then
$$a'(X) = \sum_{y < X_0} a(y) + \sum_{X_0 \le y \le X} a(y) \ge \sum_{y < X_0} a(y) + \sum_{X_0 \le y \le X} (1-\varepsilon)b(y) \ge (1-\varepsilon)b'(X) - \sum_{y < X_0} b(y)$$
Since X_0 only depends on ε, $\sum_{y<X_0} b(y) < \varepsilon b'(X)$ for large enough X. Thus, $a'(X) \ge (1-2\varepsilon)b'(X)$. The reverse inequality follows similarly. $\square$

(iv) The converse to (iii).

Proof. False. Consider $a(X) = X$ whereas $b(X) = \begin{cases} 0 & \text{if } X = 2^k, k \in \mathbb{Z} \\ X & \text{otherwise} \end{cases}$. $\square$

Problem 3

Prove the following.

(i) There are infinitely many primes of the form $4k+3$.

Proof. Suppose not. Let $p_1, \dots, p_n$ be the list of all such primes and consider $N = 4p_1 \dots p_n - 1$. Since N is odd, it can only have prime factors of the form $4k+1$ or $4k+3$. But then $N \equiv 3 \pmod 4$, so it must have a prime factor of the form $4k+3$. Thus $p_i | N$ for some i. But then $4p_1 \dots p_n - N = 1$ is divisible by p_i, contradiction. □

(ii) There are infinitely many primes of the form $4k+1$. (Hint: you may wish to prove that -1 is not a quadratic residue modulo any prime $p \equiv 3 \pmod 4$.)

Proof. Suppose not. Let $p_1, \dots, p_n$ be the list of all such primes and consider $N = (2p_1 \dots p_n)^2 + 1$. Let q be a prime factor of N. Since N is odd, $q \equiv 1, 3 \pmod 4$. Notice that $(2p_1 \dots p_n)^2 \equiv -1 \pmod q$, so we must have $q \equiv 3 \pmod 4$. But then $(q-1)/2$ is odd, and so $(-1)^{(q-1)/2} \equiv -1 \pmod q$. By Euler's criterion, -1 is not a quadratic residue modulo q, contradiction. □

Problem 4

We say that an arithmetic function is *multiplicative* if $f(ab) = f(a)f(b)$ whenever $(a,b) = 1$, and *completely multiplicative* if this holds without the coprimality restriction. For each of the functions $\Lambda, \mu, \phi, \tau, \sigma$, say with proof whether or not it is (a) multiplicative or (b) completely multiplicative.

(i) Λ is not multiplicative.

Proof. Consider $a = 2$ and $b = 3$. Then $\Lambda(ab) = \Lambda(6) = 0$ whereas $\Lambda(a)\Lambda(b) = (\log 2)(\log 3) \neq 0$. □

(ii) μ is multiplicative but not completely multiplicative.

Proof. Suppose $(a,b) = 1$. Without loss of generality, assume that $p^2|a$ for some prime p. Then $p^2|ab$ and so $\mu(ab) = \mu(a)\mu(b) = 0$. Now assume $a = p_1 \dots p_k$ and $b = q_1 \dots q_l$, where p_i and q_j are distinct primes. Since $(a,b) = 1$, $p_i \neq q_j$ for all i, j. Thus $ab = p_1 \dots p_k q_1 \dots q_l$ is a product of distinct prime. It now follows that $\mu(ab) = (-1)^{k+l} = (-1)^k(-1)^l = \mu(a)\mu(b)$.

To see that μ is not completely multiplicative, consider $a = 2$ and $b = 4$. Then $\mu(ab) = \mu(8) = 0$ whereas $\mu(a)\mu(b) = (-1)(-1) = 1 \neq 0$. □

(iii) ϕ is multiplicative but not completely multiplicative.

Proof. Suppose $(a,b) = 1$. The Chinese Remainder Theorem yields a ring isomorphism $f : \mathbb{Z}/ab\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ that sends $k \in \mathbb{Z}/ab\mathbb{Z}$ to $(k \pmod a, k \pmod b)$. But then $(k, ab) = 1$ if and only if $(k,a) = 1$ and $(k,b) = 1$. Hence, f may be restricted to a group isomorphism $(\mathbb{Z}/ab\mathbb{Z})^\times \to (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times$. It now follows from the bijectivity of f that $\phi(ab) = \phi(a)\phi(b)$.

Consider $a = 2$ and $b = 6$. Then $\phi(ab) = \phi(12) = 4$ whereas $\phi(a)\phi(b) = 1 \times 2 = 2 \neq 4$. Thus ϕ is not completely multiplicative. □

(iv) τ is multiplicative but not completely multiplicative.

Proof. Suppose $(a,b) = 1$. Let S, A, B be the sets of divisors of a, b, ab respectively. Define $f : S \to A \times B$ as $f(d) = ((d,a),(d,b))$. f is well-defined as $(\cdot,\cdot)$ is well-defined. We now show that f has an inverse $g : A \times B \to S$ defined by $g(m,n) = mn$. Since $m|a$ and $n|b$, we have $mn|ab$ and so g is well-defined. Let $m \in A$ and $n \in B$, Since $(a,b) = 1$, we have $m \nmid b$ and $n \nmid a$. But then $(mn, a) = m$ and $(mn, b) = n$, so $f(g(m,n)) = f(mn) = ((mn,a),(mn,b)) = (m,n)$. For $d \in S$, let $d_1 = (d,a)$ and $d_2 = (d,b)$. Then $g(f(d)) = g(d_1,d_2) = d_1d_2$. Note that $(d_1,d_2) = 1$ as $(a,b) = 1$, so $d_1d_2|d$. Since $(a,b) = 1$ and $d|ab$, the prime powers of d cannot exceed the prime powers of a and b, respectively. But then $d|d_1d_2$ and so $d = g(f(d))$. This shows that f is a bijection, so $|S| = |A||B|$. It now follows that $\tau(ab) = \tau(a)\tau(b)$.

To see that τ is not completely multiplicative, consider $a = 2$ and $b = 4$. Then $\tau(ab) = \tau(8) = 4$ whereas $\tau(a)\tau(b) = 2 \cdot 3 = 6 \neq 4$. □

(v) σ is multiplicative but not completely multiplicative.

Proof. Suppose $(a,b) = 1$. By the bijection g defined in (iv),

$$\sigma(a)\sigma(b) = \left(\sum_{m|a} m\right)\left(\sum_{n|b} n\right) = \sum_{m|a}\sum_{n|b} g(m,n) = \sum_{d|ab} d = \sigma(ab).$$

To see that σ is not completely multiplicative, consider $a = 2$ and $b = 2$. Then $\sigma(ab) = \sigma(4) = 7$ whereas $\sigma(a)\sigma(b) = 3 \cdot 3 = 9 \neq 7$. □

Problem 5

Show that there are arbitrarily large gaps between consecutive primes by

(i) utilizing the bounds on $\pi(x)$ shown in the course;

Proof. Suppose not. Then for all n, there exists M such that $p_{n+1} - p_n \leq M$, where p_n is the n-th prime. Since $p_1 = 2$, by induction we have $p_n \leq 2 + (n-1)M$ for all n. Hence we have $\pi(p_n) \geq p_n/M + o(1)$. But then by Theorem 1.2, $\pi(p_n) \leq cp_n/\log p_n$ for some constant $0 < c < 1$. Combining the inequalities yields $cM \geq \log p_n + o(1)$, contradiction. □

(ii) considering the numbers $n! + 2, \ldots, n! + n$.

Proof. Let n be a positive integer. Consider the numbers $n! + 2, \ldots, n! + n$. For $2 \leq k \leq n$, we have $k | n! + k$, so none of these numbers is prime. That is, $n! + 2, \ldots, n! + n$ are $n - 1$ consecutive composite numbers. Thus we may find arbitrarily large gaps between consecutive primes. □

Which of the two approaches gives the better bound?

(i) yields a better bound. For any given M, (i) guarantees the existence of a prime gap of size at least M for $p_n > e^{cM}$, whereas (ii) requires $p_n > n!$.

Problem 6

Assuming the prime number theorem, show that $p_n \sim n \log n$, where p_n denotes the n^{th} prime.

Proof. By the prime number theorem $\pi(p_n) = (1 + o(1))p_n/\log p_n$. But $\pi(p_n) = n$ by definition, so $n = (1 + o(1))p_n/\log p_n$. Rearranging gives $p_n = (1 + o(1))n \log p_n$. Taking logarithms on both sides yields $\log p_n = \log n + \log\log p_n + o(1) = \log n + o(\log n) + o(1) = (1 + o(1)) \log n$. Substituting this back gives $p_n = (1 + o(1))n \log n$. $\square$

Problem 7

Denote by τ the divisor function.

(i) Show that $\tau(n) \leq 2\sqrt{n}$.

Proof. Let $n \in \mathbb{N}$. Let D be the set of divisors of n. Then for $d \in D$ we have $\min(d, n/d) \leq \sqrt{n}$. Consider $f : D \to D$ defined by $f(d) = n/d$. Then f is an involution that pairs up divisors $\leq \sqrt{n}$ with divisors $\geq \sqrt{n}$. Thus, $\tau(n) = |D| \leq 2\sqrt{n}$. □

(ii) Find a formula for τ in terms of the prime factorisation of n.

Proof. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be he prime factorisation of n. Then any divisor d of n is of the form $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, where $0 \leq \beta_i \leq \alpha_i$ for all $1 \leq i \leq k$. Thus the number of choices for each β_i is $\alpha_i + 1$, and so there are

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$$

divisors of n. □

(iii) Using your formula from (ii), show that for any $\varepsilon > 0$ we have $\tau(n) < n^{\varepsilon}$ for sufficiently large n.

Proof. Fix $\varepsilon > 0$. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be the prime factorisation of n. Consider the ratio $\tau(n)/n^{\varepsilon}$. By (ii),

$$\frac{\tau(n)}{n^{\varepsilon}} = \prod_{i=1}^{k} \frac{\alpha_i + 1}{p_i^{\varepsilon \alpha_i}}.$$

Put $\varepsilon' = \epsilon/2$. If $p_i > 2^{1/\varepsilon'}$, then $p_i^{\varepsilon'} > 2$ and so

$$\frac{\alpha_i + 1}{p_i^{\varepsilon' \alpha_i}} < \frac{\alpha_i + 1}{2^{\alpha_i}} < 1.$$

Now suppose $p_i \leq 2^{1/\varepsilon'}$. Since $p_i^{\varepsilon} > 1$, we have

$$\frac{\alpha_i + 1}{p_i^{\varepsilon' \alpha_i}} \leq \frac{\alpha_i + 1}{2^{\varepsilon' \alpha_i}} \to 0,$$

as $\alpha \to \infty$. Hence $\frac{\alpha_i+1}{p_i^{\varepsilon' \alpha_i}} < C_i$ for some constant C_i. Since there are only finitely many such p_i,

$$C = \prod_{p_i \leq 2^{1/\varepsilon'}} C_i < \infty.$$

Combining both cases, we have

$$\frac{\tau(n)}{n^{\varepsilon'}} < C \prod_{p_i > 2^{1/\varepsilon'}} 1 = C.$$

Thus we now have

$$\frac{\tau(n)}{n^{\varepsilon}} = \frac{\tau(n)}{n^{\varepsilon'}} \cdot \frac{1}{n^{\varepsilon'}} < \frac{C}{n^{\varepsilon'}} \to 0,$$

as $n \to \infty$. This completes the proof. □

Problem 8

(i) Let X be an integer. Show that

$$\sum_{n \leq X} \log n = X \log X - X + O(\log X).$$

Proof. Since $\log n$ is increasing,

$$X \log X - X \leq \int_1^X \log t \, dt \leq \sum_{n \leq X} \log n \leq \int_1^X \log(t+1) \, dt = X \log X - X + O(\log X).$$

The result now follows. $\square$

(ii) Show that if X is an integer then

$$\sum_{p \leq X} \log p \left(\left\lfloor \frac{X}{p} \right\rfloor + \left\lfloor \frac{X}{p^2} \right\rfloor + \dots \right) = X \log X - X + O(\log X).$$

Proof. By Legendre's formula, $\alpha(p) = \sum_{k=1}^{\infty} \left\lfloor \frac{X}{p^k} \right\rfloor$ is the largest power of p dividing $X!$. Thus

$$\sum_{p \leq X} \log p \left(\left\lfloor \frac{X}{p} \right\rfloor + \left\lfloor \frac{X}{p^2} \right\rfloor + \dots \right) = \sum_{p \leq X} \log p^{\alpha(p)} = \log \prod_{p \leq X} p^{\alpha(p)} = \log X! = \sum_{n \leq X} \log n.$$

The result now follows from (i). $\square$

(iii) Show that the contribution from the terms $\left\lfloor \frac{X}{p^k} \right\rfloor$ with $k \geq 2$ is $O(X)$.

Proof. Let $L = \sum_{p \leq X} \log p \sum_{k=2}^{\infty} \left\lfloor \frac{X}{p^k} \right\rfloor$. Then

$$L \leq X \sum_{p \leq X} \log p \sum_{k=2}^{\infty} \frac{1}{p^k} = X \sum_{p \leq X} \frac{\log p}{p(p-1)}.$$

Since $\log p \leq p^{1/2}$ for all prime p,

$$\sum_{p \leq X} \frac{\log p}{p(p-1)} \leq \sum_{p \leq X} \frac{p^{1/2}}{p(p-1)} = \sum_{p \leq X} \frac{1}{p^{1/2}(p-1)} \leq \sum_{p \leq X} \frac{1}{p^{1+\varepsilon}} \leq \sum_{n \leq X} \frac{1}{n^{1+\varepsilon}} < \infty,$$

for some $\varepsilon > 0$. Thus $L = O(X)$. $\square$

(iv) Deduce Mertens' estimate

$$\sum_{p \leq X} \frac{\log p}{p} = \log X + O(1).$$

Explain why this remains valid even if X is not necessarily an integer.

Proof. Since $| \left\lfloor \frac{X}{p} \right\rfloor \log p - \frac{X \log p}{p} | \leq \log p$, by (ii) and (iii)

$$X \sum_{p \leq X} \frac{\log p}{p} + O(X) = \sum_{p \leq X} \log p \left\lfloor \frac{X}{p} \right\rfloor = X \log X + O(X).$$

Dividing both sides by X gives the result. $\square$

Problem 9

Prove the second Mertens estimate:

$$\sum_{p \le X} \frac{1}{p} = \log\log X + O(1).$$

(Hint: Write $F(y) = \sum_{p \le y} \frac{\log p}{p}$ and consider $\int_2^x F(y)w(y)dy$ for an appropriate weight function w.)

Deduce that there are constants $c_1, c_2 > 0$ such that

$$\frac{c_1}{\log X} \le \prod_{p \le X} \left(1 - \frac{1}{p}\right) \le \frac{c_2}{\log X}.$$

Proof. □

Problem 10

Let p_n denote the n^{th} prime.

(i) Is it the case that, for sufficiently large n, the sequence $p_{n+1} - p_n$ is strictly increasing?

(ii) Is it the case that, for sufficiently large n, the sequence $p_{n+1} - p_n$ is nondecreasing?

Proof. $\square$