Math 1100 — Calculus, HW #4 — Due Friday, April 9, 2010

Analytic Number Theory

Solutions

'Common mistakes' are indicated in your marked assignment with circled numbers, e.g. ①, ②, ③, etc. These labels are explained in the remarks following the solutions to each question.

Let $\mathbb{N} = \{1, 2, 3, \ldots\}$ be the set of natural numbers. *Number theory* is the study of the arithmetic structure of $\mathbb{N}$; it is very important in the design of public key cryptosystems.

For any $n, m \in \mathbb{N}$, we say that n ***divides*** m if there is some $q \in \mathbb{N}$ such that $m = n\,q$. For example, 2 divides 6 because $6 = 2 \cdot 3$. However, 2 does not divide 7. Note that 1 divides every number.

Let $p \in \mathbb{N}$, with $p \geq 2$. We say p is ***prime*** if the only numbers dividing p are 1 and p itself. For example, 2 is prime, 3 is prime, 5 is prime, and 7 is prime. However, 4, 6, 8, and 9 are *not* prime (because $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $8 = 2 \cdot 4$, $9 = 3 \cdot 3$, etc.). Let $\mathbb{P} := \{2, 3, 5, 7, 11, 13, 17, \ldots\}$ be the set of prime numbers. The ***Fundamental Theorem of Arithmetic*** says that every natural number can be written in a *unique* way as a product of primes. That is: for any $n \in \mathbb{N}$, there exist primes $p_1 < p_2 < \cdots < p_J \in \mathbb{P}$ and exponents $k_1, k_2, \ldots, k_J \in \mathbb{N}$ such that

$$n \quad = \quad p_1^{k_1} \cdot p_2^{k_2} \cdots p_J^{k_J}. \tag{1}$$

Furthermore, for each $n \in \mathbb{N}$, there is only *one* choice of primes $p_1 < p_2 < \cdots < p_J \in \mathbb{P}$ and exponents $k_1, k_2, \ldots, k_J \in \mathbb{N}$ such that (1) is true. The prime factorization (1) acts as a kind of 'fingerprint' for the number n. For this reason, prime numbers are of central importance in number theory and cryptography.[1]

$(\frac{10}{100})$ 1. Let $p \in \mathbb{N}$ and let $s > 0$ be any real number. Show that $\displaystyle\frac{1}{1 - p^{-s}} \quad = \quad \sum_{n=0}^{\infty} \frac{1}{p^{sn}}$.

Solution: The Geometric Series Identity says that, for any $x \in \mathbb{R}$ with $|x| < 1$, we have

$$\sum_{n=0}^{\infty} x^n \quad = \quad \frac{1}{1 - x}.$$

If $s > 0$, then $p^s > 1$, so $\dfrac{1}{p^s} < 1$. Setting $x := \dfrac{1}{p^s}$, we get: $\displaystyle\sum_{n=0}^{\infty} \left(\frac{1}{p^s}\right)^n \quad = \quad \frac{1}{1 - \frac{1}{p^s}}$, as desired.

□

$(\frac{10}{100})$ 2. Let $\displaystyle\left(\sum_{n=0}^{\infty} a_n\right)$ and $\displaystyle\left(\sum_{n=0}^{\infty} b_n\right)$ be two absolutely convergent series. Show that

$$\left(\sum_{n=0}^{\infty} a_n\right) \cdot \left(\sum_{m=0}^{\infty} b_m\right) \quad = \quad \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} a_n \cdot b_m.$$

[1] For example: the *RSA cryptosystem* uses the special properties of numbers of the form $p\,q$, where p and q are two very large prime numbers. RSA is used to make secure electronic transactions on the internet. You use RSA every time you buy something from Amazon.

Solution:

$$\left(\sum_{n=0}^{\infty} a_n\right)\cdot\left(\sum_{m=0}^{\infty} b_m\right) \quad = \quad \sum_{n=0}^{\infty}\left(a_n \cdot \sum_{m=0}^{\infty} b_m\right) \quad = \quad \sum_{n=0}^{\infty}\left(\sum_{m=0}^{\infty} a_n \cdot b_m\right) \quad = \quad \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} a_n \cdot b_m.$$

□

($\frac{10}{100}$) 3. Let $\mathbb{N}_{2,3}$ be the set of all natural numbers formed by multiplying a power of 2 and a power of 3. That is: $\mathbb{N}_{2,3} = \{2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 27, 32, \ldots\}$. Combine #1 and #2 to show, for all $s > 0$, that

$$\left(\frac{1}{1-2^{-s}}\right)\cdot\left(\frac{1}{1-3^{-s}}\right) \quad = \quad \sum_{n\in\mathbb{N}_{2,3}} \frac{1}{n^s}$$

$$= \quad 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \frac{1}{9^s} + \frac{1}{12^s} + \frac{1}{16^s} + \frac{1}{18^s} + \frac{1}{24^s} + \frac{1}{27^s} + \frac{1}{32^s} + \cdots\cdots$$

Solution:

$$\left(\frac{1}{1-2^{-s}}\right)\cdot\left(\frac{1}{1-3^{-s}}\right) \quad \underset{\#1}{=} \quad \left(\sum_{n=0}^{\infty} \frac{1}{2^{sn}}\right)\cdot\left(\sum_{m=0}^{\infty} \frac{1}{3^{sm}}\right)$$

$$\underset{\#2}{=} \quad \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} \frac{1}{2^{sn}}\cdot\frac{1}{3^{sm}} \quad = \quad \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} \frac{1}{(2^n 3^m)^s} \quad = \quad \sum_{n\in\mathbb{N}_{2,3}} \frac{1}{n^s}.$$

□

4. For any $J \in \mathbb{N}$, let $\mathbb{P}_J$ be the set of the first J prime numbers, and define

$$\zeta_J(s) \quad := \quad \prod_{p\in\mathbb{P}_J}\left(\frac{1}{1-p^{-s}}\right).$$

For example, $\mathbb{P}_7 = \{2, 3, 5, 7, 11, 13, 17\}$, so $\quad \zeta_7(s) \; =$

$$\left(\frac{1}{1-2^{-s}}\right)\cdot\left(\frac{1}{1-3^{-s}}\right)\cdot\left(\frac{1}{1-5^{-s}}\right)\cdot\left(\frac{1}{1-7^{-s}}\right)\left(\frac{1}{1-11^{-s}}\right)\left(\frac{1}{1-13^{-s}}\right)\left(\frac{1}{1-17^{-s}}\right).$$

($\frac{10}{100}$) Let $\mathbb{N}_J$ be the set of all natural numbers formed by multiplying powers of the first J prime numbers. (For example, $\mathbb{N}_7$ is the set of all products of any powers of 2, 3, 5, 7, 11, 13, and 17). By generalizing the argument from question #3, one can show that

$$\zeta_N(s) \quad = \quad \sum_{n\in\mathbb{N}_J} \frac{1}{n^s}, \qquad \text{for all } s > 0.$$

(You can just assume this statement.) The *Riemann Zeta Function* is defined:

$$\zeta(s) \quad := \quad \lim_{J\to\infty} \zeta_J(s) \quad = \quad \prod_{p\in\mathbb{P}}\left(\frac{1}{1-p^{-s}}\right), \tag{2}$$

for any $s \in \mathbb{R}$ where this limit exists. Find a formula for $\zeta(s)$ as a familiar infinite series. (*Hint:* Use the Fundamental Theorem of Arithmetic). Using your formula, conclude that the limit (2) converges to a finite value if $s > 1$, but the limit (2) diverges to infinity if $s \leq 1$. [2]

Solution:

$$\zeta(s) \quad = \quad \lim_{J\to\infty} \zeta_J(s) \quad = \quad \lim_{J\to\infty} \sum_{n\in\mathbb{N}_J} \frac{1}{n^s} \quad \underset{(*)}{=} \quad \boxed{\sum_{n=1}^{\infty} \frac{1}{n^s}}.$$

To see $(*)$, observe that the Fundamental Theorem of Arithmetic says: for every $n \in \mathbb{N}$, there is some J such that $n \in \mathbb{N}_J$.

Finally, note that the series is a 'p-series' (where $p = s$). We know from §11.3 that this series converges if and only if $s > 1$. □

$\left(\frac{15}{100}\right)$ 5. Let $\mathbb{M}$ be the set of all natural numbers which are *not* divisible by 2, 3, or 5 . (That is: $\mathbb{M} = \{1, 7, 11, 13, 14, 17, 23, 29, 31, 37, 41, 43, 47, 49, \ldots\}$.) In particular, observe that $\mathbb{M}$ contains 31, 61, 91, 121, and in general, all numbers of the form $30 \cdot k + 1$, for any $k \in \mathbb{N}$. Deduce that the series $\displaystyle\sum_{m\in\mathbb{M}} \frac{1}{m}$ *diverges.*

Solution: $\mathbb{M}$ contains the set $\{30 \cdot k + 1 \ ; \ k \in \mathbb{N}\}$. Thus,

$$\sum_{m\in\mathbb{M}} \frac{1}{m} \quad \geq \quad \sum_{k=1}^{\infty} \frac{1}{30k+1} \quad \geq \quad \sum_{k=1}^{\infty} \frac{1}{30k+30} \quad = \quad \sum_{k=1}^{\infty} \frac{1}{30(k+1)}$$
$$= \quad \sum_{j=2}^{\infty} \frac{1}{30j} \quad = \quad \frac{1}{30} \sum_{j=2}^{\infty} \frac{1}{j} \quad \underset{(*)}{=} \quad \infty,$$

where $(*)$ is because the Harmonic Series diverges. Thus, the Comparison Test implies that $\displaystyle\sum_{m\in\mathbb{M}} \frac{1}{m}$ diverges. □

6. Let $\{p_1, p_2, p_3, p_4, \ldots\}$ be the sequence of prime numbers (thus, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, etc.). Consider the series $\displaystyle\sum_{j=4}^{\infty} \frac{1}{p_j} \;=\; \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \cdots$.

Suppose that this series converges to some finite value α. Show that $\alpha \geq 1$.

(*Hint.* Suppose $0 < \alpha < 1$. Use question #2 and the Fundamental Theorem of Arithmetic to show

$\left(\frac{20}{100}\right)$ that $\displaystyle\sum_{n=0}^{\infty} \alpha^n \;=\; \sum_{m\in\mathbb{M}} \frac{1}{m}$. Now derive a contradiction from #5.)

---

[2] This formula was discovered by Leonhard Euler around 1740. In 1859, Bernhard Riemann showed how to extend ζ to a function defined on the complex numbers. He then showed that the distribution of prime numbers in $\mathbb{N}$ is closely related to the locations of the *zeros* of ζ in the complex plane, and he formed a conjecture about the locations of these zeros. This is the famous *Riemann Hypothesis.* One hundred and fifty years later, we still cannot either prove or disprove the Riemann Hypothesis; it is perhaps the most important unsolved problem in analytic number theory.

Solution: Suppose $0 < \alpha < 1$. Then the geometric series $\sum_{n=0}^{\infty} \alpha^n$ converges. But

$$\alpha^2 \quad = \quad \left(\sum_{j=4}^{\infty} \frac{1}{p_j} \right)^2 \quad = \quad \left(\sum_{i=4}^{\infty} \frac{1}{p_i} \right) \cdot \left(\sum_{j=4}^{\infty} \frac{1}{p_j} \right) \quad = \quad \sum_{i,j=4}^{\infty} \frac{1}{p_i \, p_j},$$

and likewise,

$$\alpha^3 \quad = \quad \left(\sum_{j=4}^{\infty} \frac{1}{p_j} \right)^3 \quad = \quad \left(\sum_{i=4}^{\infty} \frac{1}{p_i} \right) \cdot \left(\sum_{j=4}^{\infty} \frac{1}{p_j} \right) \cdot \left(\sum_{k=4}^{\infty} \frac{1}{p_k} \right) \quad = \quad \sum_{i,j,k=4}^{\infty} \frac{1}{p_i \, p_j \, p_k},$$

and more generally, for any $N \in \mathbb{N}$,

$$\alpha^N \quad = \quad \left(\sum_{j=4}^{\infty} \frac{1}{p_j} \right)^N \quad = \quad \sum_{i_1, i_2, \ldots, i_N = 4}^{\infty} \frac{1}{p_{i_1} p_{i_2} \cdots p_{i_N}}.$$

However, the Fundamental Theorem of Arithmetic implies that every element $m \in \mathbb{M}$ can be written in exactly *one* way as a $m = p_{i_1} p_{i_2} \cdots p_{i_N}$ for some $i_1, i_2, \ldots, i_N \geq 4$. Thus,

$$\sum_{N=0}^{\infty} \alpha^N \quad = \quad \sum_{N=0}^{\infty} \sum_{i_1, i_2, \ldots, i_N = 4}^{\infty} \frac{1}{p_{i_1} p_{i_2} \cdots p_{i_N}} \quad = \quad \sum_{m \in \mathbb{M}} \frac{1}{m}.$$

But from question #5, we know that $\sum_{m \in \mathbb{M}} \frac{1}{m} = \infty$. It follows that $\sum_{N=0}^{\infty} \alpha^N = \infty$. But this means that $\alpha \geq 1$. Contradiction. □

7. Consider the series

$$\sum_{n=1}^{\infty} \frac{1}{p_n} \quad = \quad \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \cdots \tag{3}$$

$\left(\frac{10}{100}\right)$ By generalizing #6, one can show that, for *any* $N \in \mathbb{N}$, if the series $\sum_{j=N}^{\infty} \frac{1}{p_j}$ converges at all, then it must converge to some $\alpha \geq 1$ (you can just assume this). Use this fact to deduce that, in fact, the series (3) *diverges.*

Solution: (By contradiction) Suppose $\sum_{n=1}^{\infty} \frac{1}{p_n}$ converges to some finite limit L. This means that $\lim_{N \to \infty} \sum_{n=1}^{N} \frac{1}{p_n} = L$. Thus, for every $\epsilon > 0$, there is some $N > 0$ such that $\left| L - \sum_{n=1}^{N} \frac{1}{p_n} \right| < \epsilon$. However,

$$L - \sum_{n=1}^{N} \frac{1}{p_n} \quad = \quad \left(\sum_{n=1}^{\infty} \frac{1}{p_n} \right) - \left(\sum_{n=1}^{N} \frac{1}{p_n} \right) \quad = \quad \sum_{n=N+1}^{\infty} \frac{1}{p_n}.$$

Thus, we are really saying that $\sum_{n=N+1}^{\infty} \frac{1}{p_n} < \epsilon$. But the generalization of #6 says that $\sum_{n=N+1}^{\infty} \frac{1}{p_n} > 1$ for all $N \in \mathbb{N}$. Since ϵ can be made arbitrarily small, we have a contradiction. □

$(\frac{15}{100})$ 8. Conclude that there exists some $N \in \mathbb{N}$ such that $p_n < n \log(n)^2$ for all $n \geq N$. [3]

Solution: (by contradiction) First note that:

$$\int_1^{\infty} \frac{1}{x \log(x)^2} \, dx \underset{(*)}{=} \int_1^{\infty} \frac{1}{u^2} \, du = \left. \frac{-1}{u} \right|_{u=1}^{u=\infty} = 1.$$

where $(*)$ is the substitution $u = \log(x)$ so that $du = \frac{1}{x} \, dx$.

Thus, the Integral Test implies that the series $\sum_{n=1}^{\infty} \frac{1}{n \log(n)^2}$ converges.

Now, suppose $p_n \geq n \log(n)^2$ for all $n \in \mathbb{N}$. Then $\frac{1}{p_n} \leq \frac{1}{n \log(n)^2}$ for all $n \in \mathbb{N}$. Thus, the Comparison Test implies that the series $\sum_{n=1}^{\infty} \frac{1}{p_n}$ also converges. But this contradicts the conclusion of question #7. □

[3]Note that the function $\log(n)^2$ increases quite slowly as $n \to \infty$. Thus, this result tells us that the sequence $\{p_1, p_2, p_3, \ldots\}$ increases 'just barely faster' than the sequence $\{1, 2, 3, \ldots\}$. In particular, the sequence $\{p_1, p_2, p_3, \ldots\}$ increases more slowly than the sequence $\{1^{\alpha}, 2^{\alpha}, 3^{\alpha}, \ldots\}$ for any exponent $\alpha > 1$. This has implications for the 'density' of prime numbers in $\mathbb{N}$. It suggests that the sequence of prime numbers grows roughly like $n \log(n)$. Indeed, for any $n \in \mathbb{N}$, let $\pi(n)$ be the number of primes in $[1...n]$. Thus, $\pi(n)/n$ is the 'density' of primes in $[1...n]$. The *Prime Number Theorem* states that

$$\lim_{n \to \infty} \frac{\pi(n)/n}{1/\ln(n)} = 1.$$

This means: if n is large, then roughly $1/\ln(n)$ of the numbers in $[1...n]$ are prime. This theorem was proved independently by Hadamard and de la Vallée Poussin in 1896 (the proof is very complicated).