

Homework 0 - Analytic number theory

Frank Thorne, thornef@webmail.sc.edu

Due Friday, September 26

Instructions: These problems are designed to gauge your background in analytic number theory and related topics. These problems do **not** necessarily represent material you are expected to know.

Please solve as many of these problems as you can. Please do not take more than three hours. Refer to books or notes if you must, but **no searching the internet**, that defeats the point.

Please provide partial solutions or comments if you don't know how to completely answer a problem. You will automatically get full credit on this assignment, if your effort looks reasonable.

1. Let $\pi(x)$ denote the number of primes $\leq x$. Can you prove any upper and lower bounds for $\pi(x)$?

Hints. This is not an easy question. It is very nontrivial to prove any lower bound whatsoever. You can prove trivial upper bounds without much difficulty; for example, you can show that $\pi(x) \leq \frac{x}{2} + 1$ by looking at divisibility by 2. Can you improve this into a bound of the form $\pi(x) \leq \frac{x}{g(x)}$, where $g(x)$ is a function unbounded as $x \rightarrow \infty$?

Please use asymptotic notation (big-O, \ll , \gg ; see below) if appropriate for your answer.

2. We say that $a \neq 0$ is a *quadratic residue* modulo p if there is an integer x with $x^2 \equiv a \pmod{p}$. Say (and prove) everything you can about quadratic residues (e.g. how many are there? if a and b are residues, are ab and $a + b$? etc.)

Do you think there are more quadratic residues less than $p/2$ or greater than $p/2$?

3. Consider the contour integral

$$\int_{2-i\infty}^{2+i\infty} X^s \frac{ds}{s}, \quad (1)$$

where the integral is over the line $2 + it$ in the complex plane.

Explain what the notation means (how is a *contour integral* defined?) Why does this integral converge, but not absolutely? Finally, if X is a positive real number, can you evaluate it? (hint: there are three cases)

If you have not had a course in complex variables before, then say so and attempt guesses for the first two questions. (You need a nontrivial theorem for the third.)

4. The *Möbius inversion formula* says the following. Let f and g be multiplicative functions, i.e. $f(mn) = f(m)f(n)$ if m and n are coprime. Then,

$$f(n) = \sum_{d|n} g(d) \quad (2)$$

if and only if

$$g(n) = \sum_{d|n} \mu(d) f(n/d). \quad (3)$$

Here $\mu(d)$ is the Möbius function, defined to be multiplicative, so that $\mu(p) = -1$ for any prime p , and $\mu(n) = 0$ if n is divisible by any squarefree number.

Prove this.

5. Recall that we say $f(x) \ll g(x)$ if there exist constants C and X , such that $f(x) < Cg(x)$ whenever $x > X$. We write $f(x) = O(g(x))$ to mean the same thing.

Prove the following equations:

$$1 + x + 10x^2 \ll x^3, \quad (4)$$

$$x^{100} \ll e^x, \quad (5)$$

$$\frac{1}{\sqrt{x}} + \log(x) + \exp((\log x)^{1/2}) \ll x. \quad (6)$$

In your proof you should determine values of C and X . However, (**important**) please come up with the **simplest proof**. If your value of C is $(9^{9999999999})!!!!$, then that is an explicit constant, good enough.

6. Prove that for any integers a and b , there is an integer n with $n \equiv a \pmod{13}$ and $n \equiv b \pmod{37}$. (Do not quote any theorem of which this is a special case!)
7. What do you know about analytic number theory, what do you hope to learn, and what (if anything) scares you about the subject?