Midterm (Take Home)

M555 – Number Theory I

October 16th, 2008

- You are not supposed to discuss this with *anyone*.
- You can use Ireland and Rosen and class notes, but please do not keep looking for solutions (in several books, papers, internet, etc.).
- Please, since you have some time, write your solutions neatly.
- The due date is Tuesday, 08/21 in class. [If you feel you need more time, please let me know ASAP, so that all can have the same amout of time.]

1. Let k and n be positive integers. Prove that for any possible choice of signs, the number

$$\pm\frac{1}{k} \pm \frac{1}{k+1} \pm \frac{1}{k+2} \pm \cdots \pm \frac{1}{k+n}$$

is not an integer. [**Hint:** Try to fix your proof of Problem 1.30 from Rosen and Ireland. For the ones who did not look, there was a hint at the back of the book for it.]

2. Assume the *Prime Number Theorem*, i.e., $\lim_{x\to\infty} \frac{\pi(x)}{x/\log(x)} = 1$. Prove that for all $c > 1$, there is N [depending on c] such that for all $x > N$ there is a prime number in (x, cx). [Compare with Bertrand's Postulate.]

3. Let n be a positive integer. We say that n is a *pseudoprime with respect to the base* b if $(b, n) = 1$, n is composite, and $b^{n-1} \equiv 1 \pmod{n}$.

Let $n = p_1^{e_1} \cdots p_r^{e_r}$, $r \geq 2$, be the prime decomposition of n. Find the number of incongruent bases modulo n with respect to which n is a pseudoprime. [Simplify your answer as much as possible.]

4. Remember that a *Fermat number* is a number of the form $F_m \stackrel{\text{def}}{=} 2^{2^m} + 1$. Prove that F_m, with $m \geq 1$, is prime if, and only if, $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$. [Note that this allows us to determine primality without factoring.]