Midterm (Take Home) – Solutions

M555 – Number Theory I

October 16th, 2008

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.]

Proof. Let r be the largest positive integer such that 2^r divides one of denominators above. [We shall prove 2^r divides *exactly* one of the denominators.] Now, suppose that $2^r \mid (k+i), (k+j)$, with $0 \leq i < j \leq n$. So, $2^r \mid (j-i)$, and let $q \in \mathbb{Z}$ such that $j = i + 2^r q$. Note that $q > 1$, as $j > i$. Then, $i < i + 2^r \leq j$, and hence $k + i + 2^r$ is one of the denominators above. Now, we have that $2^r \mid (k+i)$, and $2^{r+1} \nmid k+i$ [by the maximality of r]. So, $k + i = 2^r q'$ with q' odd. So, $k + i + 2^r = 2^r(q'+1)$, and since $q'+1$ is even, $2^{r+1} \mid (k+i+2^r)$, which contradicts the maximality of r. Hence, 2^r must divide exactly one of the denominators above.

Now, proceed as in the HW problem. Let S be the sum above and suppose it is in $\mathbb{Z}$. Then, consider

$$2^{r-1}S = \pm\frac{2^{r-1}}{k} \pm \frac{2^{r-1}}{k+1} \pm \frac{2^{r-1}}{k+2} \pm \cdots \pm \frac{2^{r-1}}{k+n},$$

which must also be an integer. Then, if $k+i$ is the only denominator divisible by 2^r, then $2^{r-1}/(k+i)$, after simplification, is the only fraction of $2^{r-1}S$ having the denominator divisible by 2. Thus, the sum of the other fractions is of the form a/b with b odd. Thus, by Problem 1.29 from the text book, we have that $a/b \pm 2^{r-1}/(k+i) = 2^{r-1}S \notin \mathbb{Z}$, and hence $S \notin \mathbb{Z}$.

□

2. Assume the *Prime Number Theorem*, i.e., $\lim_{x\to\infty} \dfrac{\pi(x)}{x/\log(x)} = 1$. 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.]

Proof. Let $c' = (c+1)/2$. [Hence $c' > 1$ also.] Since we have

$$\lim_{x\to\infty} \frac{\log(x)}{\log(c'x)} = 1, \qquad \lim_{x\to\infty} \frac{\pi(x)}{x/\log(x)} = 1,$$

we get:

$$\begin{aligned}
\lim_{x\to\infty} \frac{\pi(c'x)}{\pi(x)} &= \lim_{x\to\infty} \frac{\frac{\pi(c'x)}{c'x/\log(c'x)}}{\frac{\pi(x)}{c'x/\log(c'x)}} \\
&= \lim_{x\to\infty} \frac{\frac{\pi(c'x)}{c'x/\log(c'x)}}{\frac{\log(c'x)}{c'\log(x)}\frac{\pi(x)}{x/\log(x)}} \\
&= \left(\lim_{x\to\infty} c' \frac{\log(x)}{\log(c'x)}\right)\left(\lim_{x\to\infty} \frac{\frac{\pi(c'x)}{c'x/\log(c'x)}}{\frac{\pi(x)}{x/\log(x)}}\right) \\
&= c' > 1.
\end{aligned}$$

So, let $\epsilon = (c'-1)/2 > 0$. Then, there exists N such that if $x > N$, then $|\pi(c'x)/\pi(x) - c'| < \epsilon$, i.e., $c' - \epsilon < \pi(c'x)/\pi(x) < c' + \epsilon$. Since $c' - \epsilon = (c'+1)/2 > 1$, we have that if $x > N$, then $\pi(c'x) > \pi(x)$, and hence there is a prime in $(x, c'x] \subseteq (x, cx)$.

$\square$

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.]

Proof. For each i, since $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$ is cyclic, we have that there are $(n-1, \varphi(p_i^{e_i}))$ possible b_i's such that $b_i^{n-1} \equiv 1 \pmod{p_i^{e_i}}$. [This was done in class and in the text. It is a consequence of the proof of Proposition 4.2.1 from the text – as observer below the proof.]

So, we have that $b^{n-1} \equiv 1 \pmod{n}$ if, and only if, $b \equiv b_i \pmod{p_i^{e_i}}$, for some b_i such that $b_i^{n-1} \equiv 1 \pmod{p_i^{e_i}}$, for all i. Moreover, by the *Chinese Remainder Theorem*, this b is unique [for each choice of b_i's] modulo n.

Hence, there are $\prod_{i=1}^r (n-1, \varphi(p_i^{e_i})) = \prod_{i=1}^r (n-1, p_i^{e_i - 1}(p_i - 1)) = \prod_{i=1}^r (n-1, (p_i - 1))$ [as $p_i \mid n$, implies that $p_i \nmid (n-1)$].

$\square$

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.]

Proof. Suppose F_m is prime. Since $m \geq 1$, we have that $F_m \equiv 1 \pmod 4$. Hence, the law of quadratic reciprocity gives us

$$\left(\frac{3}{F_m}\right) = \left(\frac{F_m}{3}\right) = \left(\frac{(-1)^{2^m} + 1}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Thus, $3^{(F_m-1)/2} = -1$.

Now, assume that $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$. So, $3 \in (\mathbb{Z}/F_m\mathbb{Z})^\times$ [as $3^{F_m-1} \equiv 1 \pmod{F_m}$]. Moreover $|3| \mid (F_m - 1) = 2^{2^m}$ in $(\mathbb{Z}/F_m\mathbb{Z})^\times$. So, $|3| = 2^r$ for some r. But, if $r < 2^m$, we have that $3^{(F_m-1)/2} \equiv 3^{2^{2^m-1}} \equiv (3^{2^r})^{2^{2^m-1-r}} \equiv 1 \pmod{F_m}$, contradicting the initial assumption. Thus, $|3| = 2^{2^m}$, and so $\varphi(F_m) = |(\mathbb{Z}/F_m\mathbb{Z})^\times| \geq |3| = F_m - 1$. Therefore we must have that $\varphi(F_m) = F_m - 1$ and hence, F_m is prime.

$\square$