UMASS AMHERST MATH 471 FALL 2006, F. HAJIR

HOMEWORK 4: PRIME DISTRIBUTION I

This homework is due at the start of class on Monday October 16.

1. Show that in the sequence of primes, there are arbitrarily large gaps. To be more precise, let N be any positive integer. Show that there exists an integer a such that

$$a+1, a+2, a+3, \ldots, a+N$$

are all composite. (An integer is composite if it is greater than 1 and not prime). [1]

2. Let $\pi(x) = |\{2 \leq p \leq x \mid p \text{ is prime }\}|$ be the "prime-counting" function. Its value at a real number x is the number of primes not less than x. Show that $\pi(n) \leq n/2$ for all integers $n \geq 8$.

3. Show that $\pi(n) \leq n/3$ for all integers $n \geq 33$.

4. For an integer $N \geq 2$, define

$$\zeta_N(x) = \prod_{p \leq N} \frac{1}{1 - \frac{1}{p^x}}.$$

Recall the convention that $\prod_p$ always refers to a product over the prime numbers, thus $\prod_{p \leq N}$ means the product over the primes not exceeding N. Also, let $f(N) = \zeta_N(1)$.

(a) Fix an integer N and let S be the set of positive integers that are expressible as products of primes not exceeding N. Thus, if the primes not exceeding are $p_1, \ldots, p_s$, then

$$S = \{p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s} \mid a_i \geq 0, i = 1, \ldots, s\}.$$

Note that $1 \in S$ because $1 = \prod_{p \leq N} p^0$. Prove that

$$\zeta_N(x) = \sum_{n \in S} \frac{1}{n^x}.$$

Plug in $x = 1$ to get $f(N) = \sum_{n \in S} 1/n$.

Hint: use the same proof that we used in class for $\zeta(x)$ by expanding $1/(1 - 1/p^x)$ in a geometric power series.

---

[1] Hint: one way to do this is to write $a = b + 1$, so the sequence we want is $b+2, b+3, \ldots, b+(N+1)$. Now let's try to arrange so that $b+2$ is divisible by 2, $b+3$ is divisible by $3, \ldots$, $b+(N+1)$ is divisible by $N+1$. What does this mean about b? If this drives you crazy and you want a further hint, send an e-mail to Farshid.

(b) Prove that

$$\lim_{N\to\infty} f(N) = \infty.$$

(c) Show how (b) and the fact that the harmonic series diverges proves that there are infinitely many primes.

5. Suppose k, r are integers satisfying $k \geq 0$ and $0 \leq r \leq 5$.
(a) Show that if $p = 6k + r$ is a prime, then $r = 1$ or $r = 5$.
(b) Show that the set $\{6k + 1 \mid k \geq 0\}$ is closed under multiplication.
(c) Show that the set $\{6k + 5 \mid k \geq 0\}$ contains at least one prime. Then show that it contains infinitely many primes.
(d) Find integers b, r with $b \neq 2, 3, 6$ such that you can show the arithmetic progression $b + r, 2b + r, 3b + r, \ldots$ contains infinitely many primes in the same way.

Extra Credit Problems

A. Prove that there are infinitely many primes in the arithmetic progression $1, 5, 9, 13, \ldots$

B. Recall what we have learned (but not yet completely proved) about the structure of Gaussian primes. Up to multiplication by units, the Gaussian primes are of three types. First, there is one Gaussian prime of norm 2, namely $1 + i$. Then for each prime $q = 4k + 3$, q itself is a Gaussian prime (lying on the real line). For each prime $p = 4k + 1$, there are two Gaussian primes of norm p, namely $a + bi$ and $a - bi$ where $p = a^2 + b^2$ is the unique way to write p as a sum of two squares (except for exchanging a, b and changing their signs, which just corresponds to exchanging $a \pm bi$ or multiplying them by units).

The following question might be very hard. Or it might be very easy. What do you think?

(a) **Lonely Gaussian Primes** Is it true that for every positive integer M, there is a Gaussian prime π such that for all Gaussian primes $\pi' \neq \pi$, $N(\pi - \pi') > N$? Note that $N(\pi - \pi') = |\pi - \pi'|^2$ is the square of the distance between π and π'.

WARNING: I DO NOT KNOW THE ANSWER TO THE FOLLOWING QUESTION. NEITHER DOES ANYONE ELSE AS FAR AS I KNOW.

(b) **Gaussian Moats**
Here is a related question. Is there a positive integer k such that given any positive integer M, there is a path in $\mathbb{G}$ starting at 0 and taking only steps of size at most k that touch only at Gaussian primes, reach a Gaussian prime of size at least M? In other words, can you walk on Gaussian primes all the way out to infinity taking steps of bounded length?

More formally, is there a positive integer k such that given any integer M, there is a sequence of Gaussian primes $\pi_1, \pi_2, \ldots, \pi_n$ satisfying

$$|\pi_j - \pi_{j-1}| \leq k \qquad j = 2, \ldots, n,$$

and $|\pi_1| \leq k$, $|\pi_n| \geq M$?