Handout on Dirichlet's Theorem
Jan 30, 2019

The ideas we used in proving the infinitude of primes can be modified to prove infinitude of primes following a certain pattern. This result is a special case of a theorem known as Dirichlet's Theorem. I was going to prove the special case in class but now that we missed two classes, I will skip this. Instead, here's the proof for you to read at your own leisure time, if you wish to find out about this result. You are not responsible for this content as this will not be required for any homework or exam problem in the future.

Dirichlet's Theorem: If $\gcd(a, b) = 1$ for $a, b > 0$, then there are infinitely many primes of the form $a+kb$.

In other words, the claim is that there are infinitely many primes in the arithmetic progression $a + kb$.

The proof of this theorem requires some complex analysis, some analytic number theory (what we are doing currently is elementary number theory) and even a bit serious algebra. So we will skip the general proof. But a special case of this result can be proven using elementary methods.

Theorem: There are infinitely many primes of the form $4k + 3$, i.e. there are infinitely many primes that are equivalent to 3 mod 4.

proof: Suppose there are finitely many primes $p_1, p_2, \ldots, p_m$ of the form $4k + 3$. Consider

$$n = 4p_1p_2 \cdots p_m - 1\,.$$

Since $n \equiv 3 \pmod 4$ and $n > p_i$ for every i, n cannot be a prime and hence, it must be a composite number. So $n = q_1^{k_1} q_2^{k_2} \cdots q_r^{k_r}$ for some q_i, k_i where q_i are primes and $k_i > 0$.

If all $q_i \equiv 1 \pmod 4$, then $n \equiv 1 \pmod 4$, which is a contradiction. So at least one of $q_i = p_j$ for some j. But then $p_j|n$ and $p_j|4p_1p_2 \cdots p_m$, so $p_j|-1$, which is a contradiction again.

Therefore, the initial assumption must be incorrect, implying that there are infinitely many primes of the form $4k + 3$. □