Monday, November 30, 2015 5:23 PM

In class I had to follow a script. Here I am presenting the same result slightly differently.

Theorem There are infinitely many primes of the form $4k-1$.

Remark Dirichlet proved a groundbreaking result which essentially gave birth to a subject of mathematics called analytic number theory. He proved, for any $a,b \in \mathbb{Z}\setminus\{0\}$, if $\gcd(a,b)=1$, i.e. no common divisor more than 1, then there are infinitely many primes of the form $ak+b$.

Lemma 1. $\forall\, a_1,\dots,a_k \in \mathbb{Z}$,

$$\left.\begin{array}{l} a_1 \overset{4}{\equiv} 1, \\ a_2 \overset{4}{\equiv} 1, \\ \vdots \\ a_k \overset{4}{\equiv} 1, \end{array}\right\} \Rightarrow a_1 \cdot a_2 \cdot \ldots \cdot a_k \overset{4}{\equiv} 1.$$

Proof. $a_1 \cdot a_2 \cdot \ldots \cdot a_k \overset{4}{\equiv} (1)\cdot(1)\cdot \ldots \cdot (1) = 1.$ ■

Lemma 2. $\forall\, a_1,\dots,a_k \in \mathbb{Z}$,

$$\left.\begin{array}{l} 3 \nmid a_1 \\ 3 \nmid a_2 \\ \vdots \\ 3 \nmid a_k \end{array}\right\} \Rightarrow 3 \nmid a_1 \cdot a_2 \cdot \ldots \cdot a_k.$$

Proof. In the previous lecture using division algorithm we proved that $3 \nmid a \Leftrightarrow a \overset{3}{\equiv} \pm 1$.

So $3 \nmid a_i \Rightarrow a_i \overset{3}{\equiv} \pm 1 \Rightarrow a_1 \cdot a_2 \cdot \ldots \cdot a_k \overset{3}{\equiv} (\pm 1) \cdots (\pm 1) = \pm 1$

$\Rightarrow 3 \nmid a_1 \cdot a_2 \cdot \ldots \cdot a_k.$ ■

Proof of theorem Suppose to the contrary that there are only finitely many primes of the form $4k+3$. Let's list these primes: $p_1, p_2, \dots, p_n$. (This means, if p is prime and it is of the form $4k+3$, then $p = p_i$ for some i.)

Let $M = 4(p_1 \cdot p_2 \cdot \ldots \cdot p_n) - 1$. Notice that $M \overset{2}{\equiv} 1$ and so $2 \nmid M$.

Let $M = 4(p_1 \cdot p_2 \cdot \cdots \cdot p_n) - 1$. Notice that $M \overset{4}{\equiv} 1$ and so $2 \nmid M$.

And $p_i \nmid M$ for any $1 \leq i \leq n$ because $p_i \mid 4(p_1 \cdot \cdots \cdot p_n)$ and $p_i \nmid -1$.

On the other hand, M can be written as a product of primes.

Since $p_i \nmid M$ and $2 \nmid M$, all the prime factors of M are <u>odd</u> and NOT of the form $4k+3$. Hence all the prime factors of M are of the form $4k+1$. Therefore, by Lemma 1, $M \overset{4}{\equiv} 1$ which is a contradiction as $M \overset{4}{\equiv} -1$ and $-1 \overset{4}{\not\equiv} 1$. ■

<u>Remark</u>. The above technique is NOT suitable way to show there are infinitely many primes of the form $4k+1$ as

$$a_1 a_2 \overset{4}{\equiv} 1 \not\Rightarrow a_1 \overset{4}{\equiv} 1 \text{ or } a_2 \overset{4}{\equiv} 1.$$

In the above argument, it is crucial that we have:

$$a_1 a_2 \cdots a_n \overset{4}{\equiv} -1 \Rightarrow \exists i, \ a_i \overset{4}{\equiv} -1.$$

<u>Remark</u> Since $a_1 a_2 \cdots a_n \overset{3}{\equiv} -1 \Rightarrow \exists i, \ a_i \overset{3}{\equiv} -1$,

a similar argument can show that there are infinitely many primes of the form $3k-1$.