Lecture 8:

Theorem 8.1 (Euclid) There is an infinite number of primes.

Proof Suppose there are finite number of primes.

Let those primes be $p_1 = 2,\ p_2 = 3,\ p_3 = 5, \cdots p_n$

Consider the positive integer

$$P = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1$$

Since $P > 1$ $\exists$ p prime such that $p \mid P$. But since the only primes are $p_1, p_2, \cdots, p_n$, therefore p must be equal to one of these.

Hence $\quad p \mid p_1 \cdot p_2 \cdots p_n$

This gives us: $p \mid P - p_1 \cdot p_2 \cdots p_n$

i.e. $p \mid 1$

This is a contradiction and hence there cannot be finite number of primes.

Thm 8.2 If p_n is the nth prime number then $p_n \leq 2^{2^n - 1}$

Proof We will use principle of mathematical induction.

For $n=1$ $\quad p_1 = 2 \leq 2^{2^1 - 1}$

Hence for $n=1$, the inequality is true.

Suppose the inequality is true for all integers upto n i.e.

$$p_k \leq 2^{2^k - 1} \quad \forall \quad 1 \leq k \leq n$$

Therefore. $P_{n+1} \leq P_1 \cdot P_2 \cdots P_n + 1$

$$\leq 2 \cdot 2^2 \cdots 2^{2^{n-1}} + 1$$

$$= 2^{1+2+\cdots+2^{n-1}} + 1$$

$$= 2^{2^n - 1} + 1$$

i.e. $P_{n+1} \leq 2^{2^n-1} + 1 \leq 2^{2^n-1} + 2^{2^n-1} = 2^{2^n}$

Corollary 8.3 For $n \geq 1$, there are atleast $n+1$ primes less than 2^{2^n}.

Lemma 8.4 The product of two or more integers of the form $4n+1$ is of the same form.

Proof Sufficient to consider the product of two integers.

Let $k = 4n+1$ and $k' = 4m+1$

Then $k \cdot k' = (4n+1)(4m+1) = 16nm + 4n + 4m + 1$

$$= 4(4nm + n + m) + 1$$

Theorem 8.5 There are an infinite number of primes of the form $4n+3$.

Proof Suppose there exists only finite number of primes of the form $4n+3$.

Say $q_1, q_2, q_3, \ldots, q_s$.

Consider the positive integer

$$N = 4q_1q_2 \cdots q_s - 1 = 4(q_1q_2 \cdots q_s - 1) + 3$$

Let the prime factorization of N be

$$N = r_1 r_2 \cdots r_t$$

Note that N is odd (Even + 3). Hence

$$r_k \neq 2 \qquad \forall\, k = 1, 2, \ldots, t$$

Therefore each r_k is of the form ~~4k+1~~ $4n+1$ OR $4n+3$.
Since N is of the form $4n+3$, therefore atleast one r_k is of the form $4n+3$
[Otherwise N will be of the form $4n+1$ (Lemma 8.4)]

Since r_k is of the form $4n+3$, it must be equal to one of the q_js $(j = 1, \ldots, s)$ which implies $r_k \mid q_1 q_2 \cdots q_s$

$$\Rightarrow r_k \mid (N - q_1 \cdot q_2 \cdots q_s)$$

$$\Rightarrow r_k \mid 1$$

This is a contradiction since r_k is a prime.
Hence there cannot be finite primes of the form $4n+3$.

Theorem 8.6 (Dirichlet) If a and b are relatively prime positive integers, then the arithmatic progression

$$a, a+b, a+2b, a+3b, \ldots$$

contains infinitely many primes.