Fibonacci Sequence: The fibonacci sequence is a sequence of positive integers defined recursively by $f_0 = 1$, $f_1 = 1$, $f_2 = 2 \ldots$

$f_n = f_{n-1} + f_{n-2} \quad \forall n \geq 2$

Q) $\gcd(f_{n+1}, f_n) = 1$

Soln: $f_{n+1} = 1.f_n + f_{n-1}$

$f_n = 1.f_{n-1} + f_{n-2}$

$f_{n-1} = 1.f_{n-2} + f_{n-3}$

$\vdots$

$f_3 = 1.f_2 + f_1$

$f_2 = 1.f_1$

The above steps are nothing but euclid's algorithm for the gcd of f_{n+1} and f_n. Hence we can conclude that $f_1 = 1$ is the gcd, hence f_{n+1} and f_n are coprime.

Fundamental Theorem of Arithmetic

Every positive integer $n > 1$ is either a prime or a product of primes; the representation is unique apart from the order in which the factor occur.

i.e. $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}$; where p_i's are distinct primes.

Proof: ~~clearly~~ Existance: we can use induction on n. Clearly the statement is true for $n=2$, as n is a prime anyway. Suppose the statement is true for $n = 2, 3, \ldots k$. Now consider $k+1$. It is either a prime, in which case the ~~statement~~ Theorem is valid.

If $k+1$ is not prime, we have $k+1 = ab$. where $1 < a \le k$ and $1 < b \le k$. By the induction hypotheses, we both a and b can be written as a finite product of primes, giving us ab as a finite product of primes too.

Uniqueness: If possible let

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} = q_1^{f_1} q_2^{f_2} \cdots q_k^{f_k}$$

As $p_1 | n$, it divides, it divides $q_1^{f_1} q_2^{f_2} \cdots q_k^{f_k}$, and so p divides some prime q_j. We can assume if necessary by reordering the primes q_j, that p_1 divides q_1. But q_1 is ~~pri~~ a prime itself. Hence $p_1 = q_1$. If $e_1 > f_1$, then after cancelling p^{f_1} from both sides we will see that $p_1 = q_1$ divides $q_2^{f_2} \cdots q_k^{f_k}$, which will imply that the prime q_1 divides some other prime $q_j \neq q_1$, which is not possible. ~~Similar~~ Similarly $e_1 < f_1$ ~~to~~ leads to a contradiction. Hence we must have $e_1 = f_1$, so that we can cancel $p_1^{e_1}$ from both the factorizations. Now we can argue similarly for p_2, and then for its index e_2. We cannot have some prime left in one of the factorizations, as it will lead to 1 being expressed as a product of primes.

Theorem: There are infinitely many primes.

proof: If possible let there are finitely many primes $p_1, p_2, \ldots p_k$. consider $N = p_1 p_2 \cdots p_k + 1$. Now N is not divisible by any of the primes $p_1, p_2 \ldots p_k$. Hence either N is a prime or it is divisible by a prime which is not one of $p_1, p_2, \ldots p_k$. This leads to a contradiction.

Theorem: There are infinite primes of the form $4k+3$.

proof. The proof is analogous to Euler's proof for infinite primes. If possible, assume that there are only finitely many primes of the form $4k+3$. Suppose we denote $3 = p_1, p_2, \ldots p_n$. Now consider the number $N = 4p_2 \cdots p_n + 3$.

Now, $p_i \mid N$ for $i > 1$ would imply $p_i \mid 3$

which is not possible. Moreover 3|N would mean $3 | p_j$ for some $p_j > 3$ which is also not possible. Therefore, N is not divisible by any of the listed primes p_i. Therefore N is either a prime number or is divisible some prime q other than p_i's. If all the prime factors of odd ~~number~~ integer N are of the form 4k+1, then N will also be of the form 4k+1, which will clearly not the case. Therefore there must be a prime factor of N of the form 4k+3, which is not in $\{p_1, \ldots p_n\}$. **AA**