2 is the only even prime ~~number~~ number. All other prime numbers are odd.

Theorem 2.4.1 If p be a prime number and $1 \leq a < p$ then p is prime to a

Proof: Let $d = \gcd(a, p)$. Then $d \mid a$ and $d \mid p$

Since p is a prime and $d \mid p$, either $d = p$ or $d = 1$

But since $a < p$ and $d \mid a$, d cannot be p.

So, $d = 1$. So, d is prime to a.

Theorem 2.4.2 If p be a prime number and a is an integer $> p$ such that p is not a divisor of a, then p is prime to a

Proof: Let $d = \gcd(a, p)$. Then $d \mid a$ and $d \mid p$

Since p is a prime and $d \mid p$, either $d = p$ or $d = 1$

But $d \neq p$ since p is not a divisor of a

So, $d = 1$. Hence p is prime to a.

Theorem 2.4.3 If p be a prime number and a is an integer $> p$ such that p is a divisor of a, then $\gcd(a, p) = p$

Proof: Since p is a divisor of a, $a = pk$ where k is an integer. Hence $\gcd(a, p) = \gcd(pk, p)$

$p = p \gcd(k, 1) = p$

Theorem 2.4.4 If p be a prime number and $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Proof: If $p \mid a$ then the theorem is proved.

If p is not a divisor of a then $\gcd(a, p) = 1$, since 1 and p are the only divisors of p.

Since $\gcd(a, p) = 1$, $\exists$ integers u, v such that

$au + pv = 1$. Then $abu + pbv = b$

Now $p \mid ab$ and $p \mid pb$

$\Rightarrow p \mid (ab)u + (pb)v$, since u, v are integers

So, $p \mid b$

This completes the proof.

Corollary: If p be a prime and $p \mid a_1 \cdot a_2 \cdots a_n$ then $p \mid a_k$ for some k where $1 \le k \le n$

Proof: If $p \mid a_1$ we need not go further,

If p is not a divisor of a_1 then by the theorem $p \mid a_2 a_3 \cdots a_n$. If p is not a divisor of a_2 then $p \mid a_3 a_4 \cdots a_n$. Proceeding in a similar manner, in a finite number of steps we arrive at the desired result.

Theorem 2.4.5 A composite number has at least one prime factor

Proof: Let n be a composite number. Since n is not a prime, it has a positive divisor other than 1 and n.

Let S be the set of those positive divisors of n which are different from 1 and n. Then S is non-empty. By the well ordering property of the set $\mathbb{N}$, S contains a least element, say d.

Then $1 < d < n$. We prove that d is prime

If d be not a prime then d has a divisor d' other than d and 1 and $1 < d' < d < n$

But $d' | d$ and $d | n \Rightarrow d' | n$. So, $d' \in S$ and this ~~contradicts~~ contradicts that d is the least element of S.

So, d is prime and the theorem is proved.

Worked Examples 1. Prove that for $n > 3$, the integers n, $n+2$, $n+4$ can not be all primes.

Solution: Any positive integer n is one of the forms $3k$, $3k+1$, $3k+2$ where k is a positive integer or zero. If $n > 3$, then for $3k$, $k \neq 1$ and $k \neq 0$ for

$3k, 3k+1, 3k+2$.

Now, if $n = 3k$ then n is not a prime

If $n = 3k+1$, then $n+2 = 3k+1+2 = 3(k+1)$ and it is not a prime

If $n = 3k+2$, then $n+4 = 3k+2+4 = 3(k+2)$ and it is not a prime.

Thus, in any case, the integers n, $n+2$ and $n+4$ are not all primes.

---

2. p is a positive integer and p, $2p+1$, $4p+1$ are primes. Find p.

Solution: p is one of the form $3k$, $3k+1$, $3k+2$ where k is an integer

If $p = 3k+1$ then $2p+1 = 6k+3 = 3(2k+1)$ and it is not a prime

If $p = 3k+2$, then $4p+1 = 12k+9 = 3(4k+3)$ and it is not a prime

The only conclusion is $p = 3k$. Since p is a prime, $k = 1$ So, $p = 3$.

---

3. If $p \geq q \geq 5$ and p, q are both primes, prove that $24 \mid p^2 - q^2$.