1. Prove that there are infinitely many primes of the form $6n+5$.

Proof Suppose towards a contradiction that there are finitely many primes of the form $6n+5$, say

$$5 = p_0, p_1, p_2, p_3, \dots, p_k$$

Let $N = 6p_1p_2p_3\cdots p_k + 5$

For all primes not equal to 2, 3, they are of the form $6n+1$ or $6n+5$.

One can show that multiplying numbers of the form $6n+1$ together gives a number of the form $6m+1$. ~~6n+1~~

Left as exercise.

Suppose towards a contradiction that N only has prime factors of the form $6n+1$. By our previous remark, N would have to be of the form $6n+1$.
contradicting $N = 6p_1p_2\cdots p_k + 5$.

$\therefore$ N has a prime factor p of the form $6n+5$.

Case 1 $p = 5$.

$p \mid Nx - 5y \quad \forall x, y \in \mathbb{Z}$ by DIC.

Letting $x=1$, $y=1$. We get $p \mid 6p_1p_2\cdots p_k$.

We know $p \nmid 6$, $\therefore$ $p \mid p_1p_2\cdots p_k$.

$\Rightarrow$ $p \mid p_i$ for some $1 \le i \le k$ by Euclid's Lemma.
contradiction since p_i is prime and $p_i \neq 5$.

Case 2 $p>5$. By assumption $p \mid N$, $p = p_i$ $1 \le i \le k$

$p \mid N - 6p_1p_2 \cdots p_k$ $\Rightarrow$ $p \mid 6p_1p_2 \cdots p_k$

$\Rightarrow p \mid 5$ # contradiction since $p>5$.

contradiction since p is a prime of the form $6n+5$ not in our list.

$\therefore$ There are infinitely many primes of the form $6n+5$.

2. Let p be a prime. Prove that $\sqrt{p}$ is irrational.

Proof Suppose towards a contradiction that $\sqrt{p} = \frac{a}{b}$, $\gcd(a,b)=1$.

$\Rightarrow p = \frac{a^2}{b^2} \quad \Rightarrow b^2 p = a^2.$

By FTA, $b = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_N^{\alpha_N}$

$\Rightarrow b^2 = q_1^{2\alpha_1} q_2^{2\alpha_2} \cdots q_N^{2\alpha_N}$

Similarly $a^2 = q_1^{2\beta_1} q_2^{2\beta_2} \cdots q_N^{2\beta_N}$

p appears in the prime factorization of $b^2 \cdot p$ an odd number of times. But p appears an even number of times in a^2. #contradiction.

Completing the proof. $\square$

3. Prove that if 2^n-1 is prime, then n is prime.

Proof We prove the contrapositive.

Suppose n is composite, say $n = dg$, $d, g > 1$.

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

$$= (2^d - 1)(2^{d(g-1)} + 2^{d(g-2)} + \dots + 2^d + 1).$$

$$= 2^{dg-d+d} + 2^{dg-2d+d} + \dots + 2^d - 2^{dg-d} - 2^{dg-2d} - \dots - 1$$

$$= 2^{dg} - 1$$

Note that $2^d - 1 > 1$ since $d > 1$.

$\therefore$ $2^n - 1$ is composite. Completing the proof.

8. A number $n \in \mathbb{N}$ is perfect, if the sum of its divisors is $2n$.

Prove that if $k \in \mathbb{N}$ and $2^k - 1$ is prime, then

$$2^{k-1}(2^k - 1) \text{ is perfect.}$$

Proof Let $N = j \cdot p$ where $j = 2^{k-1}$, $p = 2^k - 1$

We define $\sigma : \mathbb{N} \to \mathbb{N}$ as follows:

$$\sigma(n) = \sum_{\substack{d \mid n \\ d \geq 1}} d.$$

$$\sigma(p) = \sum_{d \mid p} d = p + 1 = 2^k$$

$$\sigma(j) = \sum_{d \mid j} d = 1 + 2 + 2^2 + 2^3 + \dots + 2^{k-1}$$
$$= 2^k - 1$$

Note $2^k \cdot (2^k - 1) = 2(2^{k-1}(2^k - 1))$ which is the value we're looking for.

$$= \sigma(p)\sigma(j)$$

$N = p \cdot j$, if σ is multiplicative, then

$$\sigma(N) = \sigma(p \cdot j) = \sigma(p)\sigma(j) = 2^k(2^k - 1).$$

Lemma $\sigma(ab) = \sigma(a)\sigma(b)$ when $\gcd(a,b)=1$.

Proof Since $\gcd(a,b)=1$, ~~~~ a and b have no common divisors (this follows from GCD PF).

$$\sigma(ab) = \sum_{d \mid ab} d$$

$$= \sum_{d \mid a} d\,\sigma(b).$$

all the divisors of d are of the form $d = d_1 \cdot d_2$ where $d_1 \mid a$ and $d_2 \mid b$.

$$= \sigma(b) \sum_{d \mid a} d$$

$d_1 \sigma(b)$

$$= \sigma(b)\sigma(a).$$

$$\therefore \quad \sigma(N) = \sigma(j \cdot p) = \sigma(j)\sigma(p)$$

$$= (2^k - 1)2^k.$$

Thus $2^{k-1}(2^k - 1)$ is perfect.