I) Find all Pythagorean triples x, y, z (primitive and nonprimitive), with $x = 35$.

$x^2 + y^2 = z^2$, x odd $\Rightarrow y$ even

let $d = (\underbrace{x}_{=35}, y, z) \Rightarrow d \mid 35 \Rightarrow d \in \{1, 5, 7, 35\}$

I if $d = 1 \rightarrow \exists m, n \in \mathbb{Z}^+$: $\begin{cases} x = m^2 - n^2 = 35 \\ y = 2mn \\ z = m^2 + n^2 \end{cases}$
$m > n$
$m \not\equiv n \pmod 2$

$(m-n)(m+n) = 35 \Rightarrow \begin{cases} m - n = 1 \\ m + n = 35 \end{cases} \Rightarrow \begin{matrix} m = 18 \\ n = 17 \end{matrix} \Rightarrow \begin{cases} x = 35 \\ y = 612 \\ z = 613 \end{cases}$

$\begin{cases} m - n = 5 \\ m + n = 7 \end{cases} \Rightarrow \begin{cases} m = 6 \\ n = 1 \end{cases} \Rightarrow \begin{cases} x = 35 \\ y = 12 \\ z = 37 \end{cases}$

II if $d = 5 \Rightarrow (35, y, z) = 5 \Rightarrow (7, y', z') = 1$, $y' = \frac{y}{5}$, $z' = \frac{z}{5}$

$\Rightarrow \begin{cases} x = m^2 - n^2 = 7 \\ y' = 2mn \\ z' = m^2 + n^2 \end{cases} \Rightarrow (m-n)(m+n) = 7 \Rightarrow \begin{cases} m - n = 1 \\ m + n = 7 \end{cases} \Rightarrow \begin{matrix} m = 4 \\ n = 3 \end{matrix}$

$\Rightarrow \begin{cases} x' = 7 \\ y' = 24 \\ z' = 25 \end{cases} \Rightarrow \begin{cases} x = 35 \\ y = 120 \\ z = 125 \end{cases}$

III if $d = 7 \Rightarrow (35, y, z) = 7 \Rightarrow (5, y', z') = 1$, $y' = \frac{y}{7}$, $z' = \frac{z}{7}$

$\Rightarrow \begin{cases} x' = m^2 - n^2 = 5 \\ y' = 2mn \\ z' = m^2 + n^2 \end{cases} \Rightarrow \begin{cases} m - n = 1 \\ m + n = 5 \end{cases} \Rightarrow \begin{cases} m = 3 \\ n = 2 \end{cases} \Rightarrow \begin{cases} x' = 5 \\ y' = 12 \\ z' = 13 \end{cases} \Rightarrow$

$\Rightarrow \begin{cases} x = 35 \\ y = 84 \\ z = 91 \end{cases}$

IV if $d = 35 \Rightarrow (35, y, z) = 35 \Rightarrow (1, y', z') = 1$, $y' = \frac{y}{35}$, $z' = \frac{z}{35}$

$\Rightarrow \begin{cases} 1 = m^2 - n^2 \\ y' = 2mn \\ z' = m^2 + n^2 \end{cases} \Rightarrow m - n = m + n = 1$ no sol.

II) Find all integers x, with $\varphi(x) = 6$, where φ is the Euler function.

Assume $x = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ is the prime factorization of x

$\phi(x) = p_1^{\alpha_1 - 1} \cdots p_n^{\alpha_n - 1} (p_1 - 1) \cdots (p_n - 1) = 6$

$\Rightarrow p_i - 1 \leq 6 \ \forall i$, $p_i \leq 7 \Rightarrow p_i \in \{2, 3, 5, 7\}$

If $p = 5 \Rightarrow p - 1 = 4$ and $4 \nmid 6 \Rightarrow p_i \in \{2, 3, 7\}$

$\Rightarrow x = 2^a 3^b 7^c$

① $a, b, c > 0$, $\phi(x) = 2^{a-1} 3^{b-1} 7^{c-1} \underbrace{(2-1)}_{1} \underbrace{(3-1)}_{2} \underbrace{(7-1)}_{6} = 6$

$\Rightarrow 2^a 3^{b-1} 7^{c-1} = 1 \Rightarrow \begin{cases} a = 0 \\ b = 1 \\ c = 1 \end{cases}$ contrad no sol.

② $a, b > 0, c = 0$, $x = 2^a 3^b$, $\phi(x) = 2^{a-1} 3^{b-1} (2-1) \underbrace{(3-1)}_{2} = 6 \Rightarrow$

$\Rightarrow 2^a 3^{b-1} = 2 \cdot 3 \Rightarrow a = 1$, $b = 2 \Rightarrow x = 2 \cdot 3^2 = \boxed{18}$

③ $a, c > 0, b = 0$, $x = 2^a 7^c \Rightarrow \phi(x) = 2^{a-1} 7^{c-1} \cdot 6 = 6 \Rightarrow a = c = 1$

$\Rightarrow x = 2 \cdot 7 = \boxed{14}$

④ $b, c > 0, a = 0$, $x = 3^b 7^c$, $\phi(x) = 3^{b-1} 7^{c-1} \underbrace{(3-1)}_{2} \cdot 6 = 6$ no sol.

⑤ $a > 0, b = c = 0$, $x = 2^a$, $\phi(x) = 2^{a-1} = 6$ no sol.

⑥ $b > 0, a = c = 0$, $x = 3^b$, $\phi(x) = 3^{b-1} \cdot 2 = 6 \Rightarrow 3^{b-1} = 3 \Rightarrow b = 2$

$\Rightarrow x = 3^2 = \boxed{9}$

⑦ $c > 0, a = b = 0$, $x = 7^c$, $\phi(x) = 7^{c-1} \cdot 6 = 6 \Rightarrow c = 1$

$\Rightarrow x = 7^1 = \boxed{7}$

III) Define the Möbius function μ and prove that μ is multiplicative.

$\mu : \mathbb{Z}^+ \to \{-1, 0, 1\}$, $\mu(n) = \begin{cases} 1, \text{ if } n = 1 \\ (-1)^2, \text{ if } n = p_1 \cdots p_2, p_i \text{ primes, distinct} \\ 0, \text{ otherwise} \end{cases}$

- Let $m, n \in \mathbb{Z}^+$, $(m, n) = 1$ (say m)
  If at least one of them is 1, then $\mu(mn) = \mu(m \cdot 1) = \mu(m) \cdot 1 = \mu(m)\mu(1)$
  If both are ≥ 2 then $m = p_1^{\alpha_1} \cdots p_K^{\alpha_K}$, $n = p_{K+1}^{\alpha_{K+1}} \cdots p_{K+t}^{\alpha_{K+t}}$
  where $p_1 \cdots p_{K+t}$ are distinct primes

$mn = p_1^{\alpha_1} \cdots p_{K+t}^{\alpha_{K+t}}$

The only case when $\mu(mn)$ is not 0 is when $\alpha_1 \cdots \alpha_{K+t} = 1$

$\Rightarrow \mu(mn) = (-1)^{K+t} = (-1)^K (-1)^t = \mu(m)\mu(n)$

IV) If f is an arithmetic function such that $\frac{\sigma(n)}{n} = \sum_{d|n} f(d)$, where σ is the sum of divisors function, prove that f is multiplicative. Compute $f(8)$.

σ is multiplicative $\Rightarrow \forall (m, n) = 1$, $\frac{\sigma(mn)}{mn} = \frac{\sigma(m)\sigma(n)}{mn} \Rightarrow$

$\Rightarrow \frac{\sigma(n)}{n}$ is multiplicative $\Rightarrow \sum_{d|n} f(d)$ is multiplicative. But this is the summative function of f $\Rightarrow f$ is multiplicative

$f(1) = \frac{\sigma(1)}{1} = 1$,

$\frac{\sigma(2)}{2} = f(1) + f(2) \Rightarrow \frac{3}{2} = 1 + f(2) \Rightarrow f(2) = \frac{1}{2}$

$\frac{\sigma(4)}{4} = f(1) + f(2) + f(4) \Rightarrow \frac{7}{4} = 1 + \frac{1}{2} + f(4) \Rightarrow f(4) = \frac{1}{4}$

$\frac{\sigma(8)}{8} = f(1) + f(2) + f(4) + f(8) \Rightarrow f(8) = \frac{1}{8}$

V) If $r_1, r_2, \ldots r_n$ is a complete set of residues modulo n, prove that $\sum_{i=1}^{n} r_i \equiv \frac{n(n-1)}{2} \pmod{n}$

- $r_1, r_2, \ldots, r_n$ compl. set of res. mod n. We go modulo n
  $\Rightarrow r_1, \ldots, r_n$ are congruent modulo n to $0, 1, \ldots, n-1$ (in some order)

$$\Rightarrow \sum_{i=1}^{n} r_i \equiv \sum_{k=0}^{n-1} k \pmod{n} \equiv \frac{(n-1)n}{2} \pmod{n}$$

VI) If the Mersenne number $M_n = 2^n - 1$ is prime, prove that n is prime. Is the converse true? Justify your answer.

- If, by contradiction, n is composite $\Rightarrow n = ab$, $1 < a, b < n$

$$\Rightarrow M_n = 2^{ab} - 1 = (2^a)^b - 1 = \underbrace{(2^a - 1)}_{a>1 \Rightarrow 2^a > 2 \Rightarrow 2^a - 1 > 1} \underbrace{\left[(2^a)^{b-1} + \ldots + 1\right]}_{>1}$$

$\Rightarrow M_n$ is composite, contrad $\Rightarrow n$ is prime

- The converse is not true, as $M_{11} = 2^{11} - 1 = 23 \times 89$ is not prime, although $p = 11$ is prime

VII) Prove that there are infinitely many primes p of the form $p = 6k + 5$.

Assume, by contrad., that there are only finitely many primes of the form $6k+5$, say $\{p_1, \dots, p_n\}$.

Take $N = 6p_1 \cdots p_n + 5 > p_1, \dots, p_n \Rightarrow N$ is composite $\Rightarrow N$ has a prime divisor. This divisor is either of the form $6k+1$ or $6k+5$

But it cannot be $6k+5$, since not p_i divides N

(otherwise, $p_i \mid N \Rightarrow p_i \mid 5$ contrad)

$\Rightarrow N$ has only prime divisors of the form $6k+1 \Rightarrow$

$\Rightarrow N = q_1 \cdots q_t$, $q_i = 6k_i + 1 \Rightarrow N \equiv 1 \pmod 6 \Rightarrow$

$\Rightarrow 1 \equiv 5 \pmod 6$ contrad. $\Rightarrow$ the set of primes of the form $6k+5$ is infinite

VIII) If p and q are primes greater than 3, prove that $24 | (p^2 - q^2)$.

- p, q are odd numbers;
- $p = 3k \pm 1$, $q = 3\alpha \pm 1 \Rightarrow p^2 - q^2 = (9k^2 \pm 6k + 1) - (9\alpha^2 \pm 6\alpha + 1) \Rightarrow$
  $\Rightarrow 3 \mid (p^2 - q^2)$
- $p = 4k \pm 1$, $q = 4\alpha \pm 1 \Rightarrow p^2 - q^2 = (16k^2 \pm 8k + 1) - (16\alpha^2 \pm 8\alpha + 1) \Rightarrow$
  $\Rightarrow 8 \mid (p^2 - q^2)$
- $(3, 8) = 1 \Rightarrow 24 \mid (p^2 - q^2)$