I) Find all primitive and nonprimitive Pythagorean triples (x, y, z), where x or y equals 12.

Assume that $y = 12$, let $d = (x, 12, z) \Rightarrow d \in \{1, 2, 3, 4, 6, 12\}$

I. if $d = 1 \Rightarrow \exists m, n \in \mathbb{Z}^+$, $m > n$, $(m, n) = 1$; $m \not\equiv n \pmod 2$

$$\begin{cases} x = m^2 - n^2 \\ 12 = 2mn \Rightarrow mn = 6 \\ z = m^2 + n^2 \end{cases}$$

$m = 6;\ n = 1 \Rightarrow \boxed{(35, 12, 37)}$

or

$m = 3,\ n = 2 \Rightarrow \boxed{(5, 12, 13)}$

II. if $d = 2 \Rightarrow x = 2x'$, $y = 2 \cdot 6$, $z = 2 \cdot z'$; $(x', 6, z') = 1 \Rightarrow$ Pyth triple

$$\begin{cases} x' = m^2 - n^2 \\ 6 = 2mn \Rightarrow mn = 3 \text{ no sol.} \\ z' = m^2 + n^2 \end{cases}$$

III. if $d = 3 \Rightarrow x = 3x'$, $y = 3 \cdot 4$, $z = 3z'$; $(x', 4, z') = 1 \Rightarrow$ Pyth. tr.

$$\begin{cases} x' = m^2 - n^2 \\ 4 = 2mn \Rightarrow mn = 2 \Rightarrow m = 2,\ n = 1 \\ z' = m^2 + n^2 \end{cases}$$

$\Rightarrow (x', 4, z') = (3, 4, 5) \Rightarrow (x, y, z) = \boxed{(9, 12, 15)}$

IV. if $d = 4 \Rightarrow \begin{cases} x = 4x' \\ y = 4 \cdot 3 \text{ odd} \\ z = 4 \cdot z' \end{cases} \Rightarrow x'$ even $\Rightarrow \begin{cases} x' = 2mn \\ 3 = m^2 - n^2 \Rightarrow m = 2, n = 1 \\ z' = m^2 + n^2 \end{cases}$

$\Rightarrow (x', 3, z') = (4, 3, 5) \Rightarrow (x, y, z) = \boxed{(16, 12, 20)}$

V. if $d = 6 \Rightarrow \begin{cases} x = 6x' \\ y = 6 \cdot 2 \\ z = 6z' \end{cases}$; $(x', 2, z') = 1$ $\begin{cases} x' = m^2 - n^2 \\ 2 = 2mn \Rightarrow mn = 1 \text{ no sol} \\ z' = m^2 + n^2 \end{cases}$

VI. if $d = 12 \Rightarrow \begin{cases} x = 12x' \\ 12 = 12 \cdot 1 \text{ odd} \\ z = 12z' \end{cases} \Rightarrow x'$ even $\begin{cases} x' = 2mn \\ 1 = m^2 - n^2 \\ z' = m^2 + n^2 \end{cases}$ no sol.

II) If we know that there are 5 solutions to $\varphi(x) = 20$, then find 4 of them.

- $x = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, p_i's distinct primes
- $\varphi(x) = p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1}(p_1 - 1)\cdots(p_k - 1) = 20 \Rightarrow p_i \leq 21 \Rightarrow p_i \in \{2, 3, 5, 7, 11, 13, 17, 19\}$
- if $p = 7$ or $p = 13$ or $p = 19 \Rightarrow p - 1 \equiv 0 \pmod 3$ so $\varphi(x) \neq 20$
- if $p = 17 \Rightarrow p - 1 = 16 \equiv 0 \pmod 8$, so $\varphi(x) \neq 20$

$\Rightarrow p \in \{2, 3, 5, 11\}$

- 5 and 11 cannot be both in the fact of x; as $(5-1)(11-1) = 40$, so $\varphi(x) \neq 20$

Take $x = 2^a 3^b 5^c 11^d$ (at least one of c and d must be 0)

~~If $x = 2^a 3^b 5^c$, $\varphi(x) = 2^{a-1} 3^{b-1} 5^{c-1} \cdot 1 \cdot 2 \cdot 4$~~

- 3 and 5 cannot be both in the fact of x: as $(3-1)(5-1) = 8$, so $\varphi(x) \neq 20$
(that is at least one of b and c must be 0)

- if $x = 2^a \cdot 5^c \Rightarrow \varphi(x) = 2^{a-1} 5^{c-1} \cdot 1 \cdot 4 = 20 \Rightarrow 2^{a+1} \cdot 5^{c-1} = 2^2 \cdot 5 \Rightarrow a = 1, c = 2$

$\Rightarrow x = 2 \cdot 5^2$, $\boxed{x = 20}$

- if $x = 2^a \cdot 11^d \Rightarrow \varphi(x) = 2^{a-1} \cdot 11^{d-1} \cdot 1 \cdot 10 = 20 \Rightarrow 2^{a-1} \cdot 11^{d-1} = 2 \Rightarrow a = 2, d = 1$

$\Rightarrow x = 2^2 \cdot 11$, $\boxed{x = 44}$

- if $x = 3^b \cdot 11^d \Rightarrow \varphi(x) = 3^{b-1} \cdot 11^{d-1} \cdot 2 \cdot 10 = 20 \Rightarrow 3^{b-1} \cdot 11^{d-1} = 1 \Rightarrow b = 1; d = 1$

$\Rightarrow x = 3 \cdot 11$, $\boxed{x = 33}$

- if $x = 2^a \cdot 3^b \cdot 11^d \Rightarrow \varphi(x) = 2^{a-1} \cdot 3^{b-1} \cdot 11^{d-1} \cdot 1 \cdot 2 \cdot 10 = 20 \Rightarrow 2^{a-1} \cdot 3^{b-1} \cdot 11^{d-1} = 1 \Rightarrow a = b = d = 1$

$\Rightarrow x = 2 \cdot 3 \cdot 11$, $\boxed{x = 66}$

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

$$\mu(n) = \begin{cases} 1, & \text{if } n=1 \\ (-1)^k, & \text{if } n = p_1 \cdots p_k, \ p_i \text{ distinct primes} \\ 0, & \text{otherwise} \end{cases}$$

Let $m, n \in \mathbb{Z}^+$, $(m,n)=1$. if $m=1$, or $n=1$, then $\mu(m\cdot 1) = \mu(m) = \mu(m)\mu(1)$ ✓

- If $m, n > 1$, then the only case in which $\mu \neq 0$ is when neither m nor n are divisible by a square of prime.

$m = p_1 \cdots p_k$; $n = q_1 \cdots q_s$, where $p_1, \ldots, p_k, q_1, \ldots, q_s$ are distinct primes

$\Rightarrow \mu(mn) = (-1)^{k+s} = (-1)^k \cdot (-1)^s = \mu(m)\mu(n)$

IV) If $p > 2$ is prime and $p = a^2 + b^2$, then show that $p \equiv 1 \pmod 4$.

$p > 2$ prime $\Rightarrow p$ is odd $\Rightarrow$ a and b cannot be both even or both odd

Assume a even $\Rightarrow a = 2k$, $k \in \mathbb{Z}$
b odd $\Rightarrow b = 2t+1$, $t \in \mathbb{Z}$

$\Rightarrow a^2 + b^2 = 4k^2 + (2t+1)^2 = 4k^2 + 4t^2 + 4t + 1 = 4(k^2 + t^2 + t) + 1$
$\equiv 1 \pmod 4$

V) What is a pseudoprime to the base b? Give an example of a pseudoprime to the base 2, showing your calculations.

• Let $b \in \mathbb{Z}^+$. if n is composite ($n \in \mathbb{Z}^+$) and $b^n \equiv b \pmod{n}$, then n is a pseudoprime to the base b

. Take $n = 341 = 11 \times 31$ composite

$$2^{10} \equiv 1 \pmod{11} \Rightarrow 2^{341} = \underbrace{(2^{10})^{34}}_{\equiv 1 \pmod{11}} 2 \equiv 2 \pmod{11}$$

$$2^{30} \equiv 1 \pmod{31} \Rightarrow 2^{341} = \underbrace{(2^{30})^{11}}_{\equiv 1 \pmod{3}} . 2^{11} \equiv 2^{11} = \underbrace{(2^5)^2}_{32 \equiv 1 \pmod{31}} . 2 \equiv 2 \pmod{31}$$

But $(11, 31) = 1 \Rightarrow 2^{341} \equiv 2 \pmod{11 \times 31}$

$$2^{341} \equiv 2 \pmod{341}$$

VI) If $n^3 - 1$ is prime, then show that $n = 2$.

$$n^3 - 1 = (n-1)(n^2+n+1) \Rightarrow n - 1 = 1 \Rightarrow n = 2$$

tion

VII) Prove that $9|(7^{53} - 4)$.

$7^3 = 343 \equiv 1 \pmod 9$

$\Rightarrow 7^{53} = \underbrace{(7^3)}_{\equiv 1 \pmod 9}{}^{17} \cdot 7^2 \equiv 49 \equiv 4 \pmod 9$

$\Rightarrow 9 | (7^{53} - 4)$

VIII) If p is prime and $k \geq 1$, then show that it is impossible for p^k to be a perfect number.

p^k is perfect if $\sigma(p^k) = 2p^k$

but $\sigma(p^k) = 1 + p + \cdots + p^k$

and if $\sigma(p^k) = 2p^k \Rightarrow 1 + p + \cdots + p^k = 2p^k$

by contrad.

$1 + p + \cdots + p^{k-1} = p^k$

$\Rightarrow p^k - p^{k-1} - \cdots - p = 1 \Rightarrow p | 1 \Rightarrow p = 1$ contradiction

$\Rightarrow p^k$ cannot be perfect