Problem 5. A positive integer N has the following properties:

(i) N is a square.

(ii) N is the sum of two positive squares in a unique way (up to order).

(iii) $\mathrm{d}(N)\phi(N) = 8N$.

Here $\mathrm{d}(N)$ is the number of positive divisors of N and ϕ is the Euler function. What is N?

Solution. We will show that $N = 2025$ is the only solution. We start by recalling the formulas for $\mathrm{d}(N)$ and $\phi(N)$. If $N = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ is the factorization of N into powers of prime numbers, where $p_1 < p_2 < \ldots < p_k$ are primes, then

$$\mathrm{d}(N) = (a_1+1)(a_2+1)\dots(a_k+1) \quad \text{and} \quad \phi(N) = \frac{N(p_1-1)(p_2-1)\dots(p_k-1)}{p_1 p_2 \dots p_k}.$$

These formulas are discussed in most elementary number theory classes or books. It follows that the equality $\mathrm{d}(N)\phi(N) = 8N$ is equivalent to

$$8p_1p_2\dots p_k = (a_1+1)(a_2+1)\dots(a_k+1)(p_1-1)(p_2-1)\dots(p_k-1). \tag{1}$$

Suppose now that N is a square. This means that all the numbers $a_1, \dots, a_k$ are even. Thus the number $(a_1+1)(a_2+1)\dots(a_k+1)$ is odd and divides $8p_1p_2\dots p_k$, so $(a_1+1)(a_2+1)\dots(a_k+1)$ is a divisor of $p_1p_2\dots p_k$, i.e

$$(a_1+1)(a_2+1)\dots(a_k+1)m = p_1p_2\dots p_k \tag{2}$$

for some positive integer m. Note that $(a_1+1)(a_2+1)\dots(a_k+1)$ is a product of at least k prime numbers (since each factor (a_i+1) contributes at least one prime number). Since on the right side of (2) we have a product of exactly k prime numbers, we must have $m = 1$ and each a_i+1 is a prime number. It follows that $(a_1+1)(a_2+1)\dots(a_k+1) = p_1p_2\dots p_k$ and $a_i + 1 = p_{\tau(i)}$ for $i = 1, \dots, k$ and some permutation τ of $1, 2, \dots, k$ Thus all the prime numbers p_i are odd. From (1) we get $8 = (p_1-1)\dots(p_k-1)$ and $1 < p_1 - 1 < \ldots < p_k - 1$. The only way to factor 8 into a product of increasing factors is 8 or $2 \cdot 4$. In the former case, we have $k = 1$ and $p_1 - 1 = 8$, which is not possible as 9 is not a prime. Thus $k = 2$, $p_1 - 1 = 2$, $p_2 - 1 = 4$. This implies that $p_1 = 3$, $p_2 = 5$ and $(a_1+1)(a_2+1) = 3 \cdot 5$. Thus either $a_1 = 2$ and $a_2 = 4$ or $a_1 = 4$ and $a_2 = 2$. We see that either $N = 3^2 \cdot 5^4$ or $N = 3^4 \cdot 5^2$.

Summarizing our discussion so far, we proved that N satisfies (i) and (iii) if and only if either $N = 3^2 \cdot 5^4 = 5625$ or $N = 3^4 \cdot 5^2 = 2025$. However

$$5625 = 21^2 + 72^2 = 45^2 + 60^2$$

so $N = 5625$ does not satisfy (ii). It follows that only $N = 2025$ can satisfy conditions (i)-(iii). It remains to show that 2025 indeed satisfies (ii). To this end note that if a is not divisible by 3 then $a^2 - 1$ is divisible by 3. Thus if 3 divides $a^2 + b^2$ then 3 must divide both a and b. Consequently, if $2025 = a^2 + b^2$ then $a = 9a_1$, $b = 9b_1$ and $a_1^2 + b_1^2 = 25$. It is now straightforward to see that $a_1 = 3$, $b_1 = 4$ is the only possibility (up to order), i.e. $2025 = 27^2 + 45^2$ is the only was to express 2025 as a sum of two positive squares.

Remark. Recall that triples (a, b, n) of positive integers such that $a^2 + b^2 = n^2$ are called Pythagorean triples. A classical result in elementary number theory states that every such triple is of the form

$$a = 2uwk, b = (u^2 - w^2)k, n = (u^2 + w^2)k \quad \text{or} \quad a = (u^2 - w^2)k, b = 2uwk, n = (u^2 + w^2)k$$

for some positive integers k, u, w such that u, w are relatively prime and one of u, w is even.

Another classical result in elementary number theory describes when a given number N is the sum of two squares. We can express N in a unique way as

$$N = 2^c p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} q_1^{b_1} \dots q_m^{b_m}$$

where $p_1 < \ldots < p_k$ are odd primes of the form $4t+1$, $q_1 < \ldots < q_m$ are odd primes of the form $4t-1$, $c \geq 0$, and a_i, b_j are positive integers (we allow the possibility that there are no factors of the form p_i or q_i). Then:

- If at lest one b_i is odd then N is not the sum of two squares of integers.
- If all b_i are even then N is the sum of two squares of integers and if $N = a^2 + b^2$ then both a and b are divisible by $D = 2^{(c-e)/2} q_1^{b_1/2} \dots q_m^{b_m/2}$, where $e = 1$ if c is odd and $e = 0$ if c is even.
- The number of ways to express N as the sum of two positive squares is

$$\begin{cases} \frac{(a_1+1)(a_2+1)\dots(a_k+1)}{2} & \text{if at least one } a_i \text{ is odd} \\ e + \frac{(a_1+1)(a_2+1)\dots(a_k+1)-1}{2} & \text{if all } a_i \text{ are even.} \end{cases}$$

- To enumerate all expressions $N = a^2 + b^2$ use the following procedure. Let $D = 2^{(c-e)/2} q_1^{b_1/2} \dots q_m^{b_m/2}$. Write $p_j = u_j^2 + w_j^2$ (it is unique up to order). Choose integers $0 \le m_j \le a_j$ for every j. Consider the complex number

$$(u_1 + iw_1)^{m_1}(u_1 - iw_1)^{a_1 - m_1} \dots (u_k + iw_k)^{m_k}(u_k - iw_k)^{a_k - m_k}(1 + i)^e$$

(here $i^2 = -1$). It is of the form $A + Bi$ for some integers A, B. Then $(D|A|)^2 + (D|B|)^2 = N$. Two choices $m_1, \dots, m_k$ and $m_1', \dots, m_k'$ lead to the same expression (up to order) if and only if $m_j' = a_j - m_j$ for all j. One of A, B is 0 if and only if $e = 0$, all a_i are even and $m_j = a_j/2$ for all j. All ways to write $N = a^2 + b^2$ are of this form.

Example. As an example consider $N = 5625 = 3^2 \cdot 5^4$. Thus $p_1 = 5$, $a_1 = 4$, $q_1 = 3$, $b_1 = 2$, $e = 0$, $D = 3$. According to our formula, 5625 has $(3-1)/2 = 2$ expressions as the sum of 2 positive squares. To find them we follow the enumeration process outlined above. We have $p_1 = 5 = 2^2 + 1^2$. When we take $m_1 = 4$ we get the complex number $(2 + i)^4 = 16 + 32i - 24 - 8i + 1 = -7 + 24i$ which yields $5625 = (7D)^2 + (24D)^2 = 21^2 + 72^2$. The same decomposition is obtained when $m_1 = 0$. Taking $m_1 = 1$ leads to $(2 + i)(2 - i)^3 = 5(2 - i)^2 = 15 - 20i$, so $5625 = (15D)^2 + (20D)^2 = 45^2 + 60^2$. Taking $m_1 = 3$ yields the same decomposition. Finally, taking $m_2 = 2$ we get $(2 + i)^2(2 - i)^2 = 25 + 0i$, so $5625 = 75^2 + 0^2$.

Problem. Find all positive integers N which satisfy (iii). Which of them also satisfy (ii)?