Answer on Question #58504 – Math – Combinatorics | Number Theory

Question

Suppose a prime can be written as $p = x^2 + 5y^2$. Show that $p \equiv 1$ or 9 (mod 20).
Assume that $p > 5$.

Solution

Because p is a prime, p cannot be even, hence p is odd.
We may assume that p is an odd prime, greater than 5. Because $p = x^2 + 5y^2$ is odd, one of x^2, y^2 is odd, and the other is even.

Reducing $p = x^2 + 5y^2$ mod 5, we see $p = x^2$ (mod 5), so p is a quadratic residue mod 5 and thus p = 1 or 4 (mod 5).

Reducing $p = x^2 + 5y^2$ mod 4, we see $p = x^2 + y^2$ (mod 4), so p is a sum of two quadratic residues mod 4.
Since the quadratic residues mod 4 are 0 and 1, this rules out the possibility that p=3 (mod 4). Besides, p=0 (mod 4), p=2 (mod 4) are excluded, because p is odd.

So p = 1 or 4 (mod 5) and p = 1 (mod 4), which means that p = 1 or 9 (mod 20).
Check it.

Let

$$p = 1 + 4k \text{ and } p = 1 + 5l \text{ or } p = 4 + 5m.$$

Suppose that $p = 1 + 4k$ and $p = 1 + 5l$.
Then $1 + 4k = 1 + 5l$, $4k = 5l$, hence $k = 5t$, $l = 4u$.
This means that $p = 1 + 4k = 1 + 4 \cdot 5t = 1 + 20t$, $p = 1 + 5l = 1 + 5 \cdot 4u = 1 + 20u$.
Finally obtain p = 1 (mod 20).

Suppose that $p = 1 + 4k$ and $p = 4 + 5m$.
Then $1 + 4k = 4 + 5m$, $4k - 4 - 4m = m - 1$, $4n = m - 1$, hence $m = 4n + 1$.
This means that $p = 4 + 5m = 4 + 5 \cdot (4n + 1) = 4 + 20n + 5 = 9 + 20n$.
Finally obtain p = 9 (mod 20).

Given p = 1 or 4 (mod 5) and p = 1 (mod 4), we came to p = 1 or 9 (mod 20), which was to be proved.