EXPRESSING A NUMBER AS A SUM OF TWO SQUARES

Problem. Find the number of ways $S(n)$ in which a positive integer $n > 1$ can be represented in the form

$$n = x^2 + y^2 \qquad (x \geq y > 0).$$

Remark 1. From

$$(x+y)^2 + (x-y)^2 = 2(x^2+y^2)$$

we deduce easily that if $n = 2^e m$ then

$$S(n) = S(n/2) = S(n/4) = \cdots = S(m).$$

For example, $S(280) = S(35)$. So we can confine our attention to odd n, which we do from now on.

Remark 2. Geometrically, multiplication by i is rotation through 90 degrees. Consequently every non-zero Gaussian integer is in a unique way the product of a unit and a Gaussian integer $a + ib$ lying in the first quadrant (i.e., $a > 0$ and $b \geq 0$). As the Gaussian integers form a UFD, it follows that every non-zero non-unit Gaussian integer factors *uniquely* as a unit times a product of prime, first-quadrant Gaussian integers.

Remark 3. A key observation is that $x^2 + y^2$ is the norm $N(\xi)$ of a Gaussian integer $\xi = x + iy$, and then it is also the norm of $y + ix$. If x and y are both positive, then exactly one of these two has real part $\geq$ imaginary part. Hence if $S'(n)$ is the number of first-quadrant Gaussian integers ξ such that $N(\xi) = n$ (so that $x \neq y$ since n is odd) then we have $S'(n) = 2S(n)$ *unless* n is a square, say $n = m^2$, in which case the Gaussian integer $m + i0$ contributes 1 to $S'(n)$ but does not contribute to $S(n)$, so that $S'(n) = 2S(n) + 1$.

It is easier to work with S' than directly with S, because of the following Lemma.

Lemma. *If $n = n_1 n_2$ with $(n_1, n_2) = 1$ then every Gaussian integer ξ such that $N(\xi) = n$ factors uniquely as $\xi = u\xi_1\xi_2$ where u is a unit, ξ_1 and ξ_2 are first-quadrant Gaussian integers, $N(\xi_1) = n_1$ and $N(\xi_2) = n_2$.*

Proof. Factor ξ as in Remark 2. Let ξ_j' $(j = 1, 2)$ be the product of all the prime factors of ξ whose norm (which, recall, is either a $\mathbb{Z}$-prime $\equiv 1 \pmod 4$ or the square of a $\mathbb{Z}$-prime $\equiv 3 \pmod 4$, and is a divisor of n, hence of n_1 or n_2, but not both) divides n_j. Let ξ_j be the unique first-quadrant Gaussian integer associated to ξ_j' (i.e., equal to ξ_j' times a unit). Then $N(\xi_j v) = N(\xi_j')$ divides n_j (why?), and

$$N(\xi_1)N(\xi_2) = N(\xi) = n = n_1 n_2$$

shows that $N(\xi_j) = n_j$. This proves the existence of the asserted factorization of ξ. Uniqueness is left as an exercise.

Corollary. *If $n_1 > 1$ and $n_2 > 1$ are relatively prime then*

$$S'(n_1 n_2) = S'(n_1) S'(n_2).$$

Now factor n as

$$n = p_1^{e_1} \cdots p_r^{e_r} q_1^{f_1} \cdots q_s^{f_s} \tag{1}$$

where the p_i are distinct positive integer primes $\equiv 1 \pmod 4$ and the q_j are distinct positive integer primes $\equiv 3 \pmod 4$.

The preceding Corollary yields:

$$S'(n) = S'(p_1^{e_1}) \cdots S'(p_r^{e_r}) S'(q_1^{f_1}) \cdots S'(q_s^{f_s}). \tag{2}$$

For a prime $p \equiv 1 \pmod 4$ there are two first-quadrant Gaussian integers ξ_1 and ξ_2 having norm p, namely those which appear in the factorization of p (see Remark 2). Factoring any ξ with norm p^e as in Remark 2, we see that

$$\xi = \xi_1^g \xi_2^{(e-g)} \qquad (g = 0, 1, \ldots, e).$$

Hence

$$S'(p^e) = e + 1. \tag{3}$$

For a prime $q \equiv 3 \pmod 4$ the only first-quadrant Gaussian integer ξ having q^e as norm is $q^{(e/2)}$ (as can be seen by factoring ξ into Gaussian primes). Thus

$$S'(q^f) = \begin{cases} 1 \text{ if } f \text{ is even,} \\ 0 \text{ if } f \text{ is odd.} \end{cases} \tag{4}$$

From (2), (3), (4), and Remark 3, we conclude:

Theorem. *For n as in (1) we have $S(n) = 0$ if any f_j is odd; and if all the f_j are even then*

$$S(n) = \begin{cases} 1/2(e_1+1)(e_2+1)\cdots(e_r+1) \text{ if } n \text{ is not a square,} \\ 1/2[(e_1+1)(e_2+1)\cdots(e_r+1) - 1] \text{ if } n \text{ is a square.} \end{cases}$$

Example. If $n = p_1^2 p_2 p_3$ with distinct positive integer primes $p_i \equiv 1 \pmod 4$ then $S(n) = 6$.

The number of right-angle triangles with integer sides having hypotenuse n is $S(n^2) = 22$. (Just 4 of these have relatively prime sides—count the solutions of $n = u^2 + v^2$ with relatively prime u and v).