4. Gaussian integers

We are going to use the fact that $\mathbb{Z}[i]$ is a UFD, meaning that we can factor Gaussian integers into products of Gaussian primes and this factorisation is unique, to count the number of ways to write a natural number as a sum of squares.

Recall

Definition 4.1. *Let $a + bi \in \mathbb{Z}[i]$ be a Gaussian integer.*

*The **norm** of $a + bi$, denoted $N(a + bi)$, is $a^2 + b^2$.*

Note that the norm of $a + bi$ is the product of $a + bi$ and $a - bi$, the **conjugate** of $a + bi$.

Lemma 4.2. *The norm is multiplicative, that is,*

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Proof. This is a restatement of (2.1). □

Lemma 4.3. *The units in $\mathbb{Z}[i]$ are precisely the elements of norm 1.*

Proof. Suppose that $\alpha \in \mathbb{Z}[i]$ is a unit. Then we may find β such that $\alpha\beta = 1$ and so

$$1 = N(\alpha)N(\beta).$$

Thus $N(\alpha) = 1$.

The elements of norm 1 are ± 1 and $\pm i$. The inverse of ± 1 is ± 1 and the inverse of $\pm i$ is $\mp i$, so that elements of norm one are all units. □

Lemma 4.4. *Let $p \in \mathbb{Z}$ be a prime congruent to 3 modulo 4.*

Then p is a prime in $\mathbb{Z}[i]$.

Proof. Suppose that

$$p = (a + bi)(c + di).$$

Taking norms we see that

$$p^2 = (a^2 + b^2)(c^2 + d^2).$$

As $p \equiv 3 \mod 4$, p is not a sum of squares. Thus $a^2 + b^2 = p^2$ and $c^2 + d^2 = 1$, so that $c + di$ is a unit, or vice-versa. □

Lemma 4.5. *Let $\alpha = a + bi$ be a Gaussian integer whose norm is a prime p.*

Then α is a prime Gaussian integer.

Proof. Suppose that $\alpha = \beta\gamma$. Then

$$p = N(\beta)N(\gamma).$$

As p is prime we must have $N(\beta)$ or $N(\gamma) = 1$. But then β or γ is a unit so that α is a prime. □

Definition-Theorem 4.6. *Suppose that*

$$n = 2^u n_1 n_2$$

where n_1 is a product over primes congruent to 1 modulo four and n_2 is a product over primes congruent to 3 modulo four. If $r_2(n)$ denotes the number of representations of n as a sum of two squares then

$$r_2(n) = \begin{cases} 0 & \text{if } n_2 \text{ is not a square} \\ 4\tau(n_1) & \text{if } n_2 \text{ is a square.} \end{cases}$$

Proof. (2.3) implies that n_2 must be a square and that all representations of n as a sum of squares are induced by a multiplying a representation of $2^u n_1$ by the square root of n_1. We are also going to prove this directly.

Suppose that $n = x^2 + y^2$ is a sum of squares. Then

$$n = (x + iy)(x - iy),$$

is a product of two conjugate Gaussian integers and vice-versa. It follows that there is a correspondence between factorisations of n as products of two conjugate Gaussian integers and representations of n as a sum of two squares.

So we just have to count the number of ways to write n as a product of conjugate Gaussian integers. Suppose that

$$n_1 = \prod_{p_j \equiv 1 \mod 4} p_j^{t_j} \qquad \text{and} \qquad n_2 = \prod_{q_j \equiv 3 \mod 4} q_j^{s_j}.$$

By what we already proved, $s_j = 2r_j$ is even. Note that

$$2 = i(1 - i)^2 \qquad \text{and} \qquad p_j = (a_j + ib_j)(a_j - ib_j)$$

for some integers a_j and b_j. Thus

$$n = i^u (1 - i)^{2u} \prod((a + ib)(a - ib))^t \prod q^{2r},$$

where subscripts have been omitted for clarity and

$$a > 0, \qquad b > 0 \qquad \text{and} \qquad p = a^2 + b^2.$$

Using the fact that $\mathbb{Z}[i]$ is a UFD and the identification of Gaussian primes, it follows that the divisors of n have the form

$$x + iy = i^v (1 - i)^{u_1} \prod (a + ib)^{t_1} (a - ib)^{t_2} \prod q^{r_1},$$

up to units and re-ordering, where

$$0 \leq v \leq 3, \quad 0 \leq u_1 \leq 2u, \quad 0 \leq t_1 \leq t, \quad 0 \leq t_2 \leq t, \quad \text{and} \quad 0 \leq r_1 \leq 2r.$$

We check under what conditions n is the product of $x + iy$ and $x - iy$. Now

$$\begin{aligned} x - iy &= (-i)^v (1+i)^{u_1} \prod (a - ib)^{t_1} (a+ib)^{t_2} \prod q^{r_1} \\ &= i^{u_1 - v} (1-i)^{u_1} \prod (a+ib)^{t_2} (a-ib)^{t_1} \prod q^{r_1}. \end{aligned}$$

So we need $u_1 = u$, $t_1 + t_2 = t$, $r_1 = r$. Since there are only four distinct powers of i, the complete list is given by

$$i^v (1-i)^u \prod (a+ib)^{t_1} (a-ib)^{t-t_1} \prod q^r,$$

where u, t and r are fixed, $v \in \{ 0, 1, 2, 3 \}$ and $t_1 \in \{ 0, 1, \ldots, t \}$. The total number in this list is

$$4 \prod (t+1) = 4\tau(n_1). \qquad \square$$