5 Gaussian Integers and sums of squares

Aims of this chapter: to discover things about the arithmetic of $\mathbb{Z}$ by passing to larger number rings.

The Gaussian integers

Definition. The set of **Gaussian integers** is $\mathbb{Z}[i] = \{a + b\,i \mid a, b \in \mathbb{Z}\}$.

Remark. $\mathbb{Z}[i]$ is closed under addition and multiplication, and contains $\mathbb{Z}$: it is a subring of $\mathbb{C}$. It is not a field: dividing one Gaussian integer by another results in an element of $\mathbb{Q}(i)$ with *rational* real and imaginary parts.

Questions: What does $\mathbb{Z}[i]$ look like? Does it have an "arithmetic" like that of $\mathbb{Z}$? What are "Gaussian primes"?

Remark. Note that $(1+i)(1-i) = 2$, so the number 2 is "not prime" in $\mathbb{Z}[i]$. Neither is 5, since $5 = (1+2i)(1-2i)$. What about $3 = (-1)(-3) = i(-3i)$?

Definition. An element $\alpha \in \mathbb{Z}[i]$ is a **unit**, or **invertible element**, if there exists a $\beta \in \mathbb{Z}[i]$ such that $\alpha \cdot \beta = 1$. Two elements α and β in $\mathbb{Z}[i]$ are called **associate** to each other if $\alpha = \gamma\beta$ for some unit γ.

To answer the above questions properly we first need to decide what the units of $\mathbb{Z}[i]$ are. As well as ± 1 there are also $\pm i$ since $i(-i) = 1$. Are there any more? To decide this we'll introduce a function on $\mathbb{Z}[i]$ called the norm.

Definition. The function $\mathrm{N}\colon \mathbb{Z}[i] \to \mathbb{Z}$, called the **norm**, is defined by

$$\mathrm{N}(a+bi) = (a+bi)(a-bi) = a^2 + b^2,$$

so $\mathrm{N}(\alpha) = \alpha \cdot \overline{\alpha}$.

Lemma 5.1 (Properties of the norm).

a). $\mathrm{N}(\alpha) = 0$ *if and only if* $\alpha = 0$;

b). $\mathrm{N}(\alpha \cdot \beta) = \mathrm{N}(\alpha) \cdot \mathrm{N}(\beta)$;

c). $\mathrm{N}(\alpha) = 1$ *if and only if* α *is a unit in* $\mathbb{Z}[i]$;

d). $\{1, i, -1, -i\}$ *is the complete set of units of* $\mathbb{Z}[i]$.

Proof. a). is obvious.

b). We have
$$\mathrm{N}(\alpha \cdot \beta) = (\alpha \cdot \beta) \cdot \overline{\alpha \cdot \beta} = \alpha \cdot \overline{\alpha} \cdot \beta \cdot \overline{\beta} = \mathrm{N}(\alpha) \cdot \mathrm{N}(\beta)\,.$$

c). If $\mathrm{N}(\alpha) = 1$ then $\alpha \cdot \overline{\alpha} = 1$ and since $\overline{\alpha}$ is also in $\mathbb{Z}[i]$, we must have that α is a unit. Conversely, if $\alpha \cdot \beta = 1$ for some $\beta \in \mathbb{Z}[i]$, then $\mathrm{N}(\alpha) \cdot \mathrm{N}(\beta) = 1$ and since both $\mathrm{N}(\alpha)$ and $\mathrm{N}(\beta)$ are positive integers, we have $\mathrm{N}(\alpha) = \mathrm{N}(\beta) = 1$.

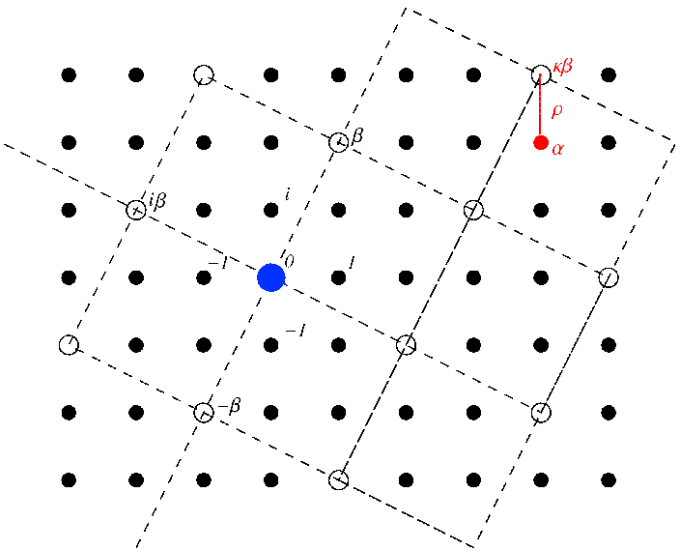
d). We find all the units by solving $\mathrm{N}(\alpha) = 1$. If $\alpha = a + b\,i$, then $a^2 + b^2 = 1$ gives that either a or b must be 0 and the other ± 1.

□

Theorem 5.2 (Euclidian division in $\mathbb{Z}[i]$). *Given α and $\beta \neq 0$ in $\mathbb{Z}[i]$, there exists κ and ρ in $\mathbb{Z}[i]$ such that*

$$\alpha = \kappa \cdot \beta + \rho \qquad \text{and} \qquad \mathrm{N}(\rho) < \mathrm{N}(\beta)\,.$$

We call κ the κuotient and ρ the ρemainder.



Proof. The vector from 0 to $i\beta$ is perpendicular to the vector from 0 to β in the complex plane $\mathbb{C} = \mathbb{R}^2$. So the set

$$\beta \cdot \mathbb{Z}[i] = \{\kappa \cdot \beta \mid \kappa \in \mathbb{Z}[i]\}$$

forms a lattice of squares with side length $|\beta| = \sqrt{\mathrm{N}(\beta)}$. Our given α belongs to at least one of these squares. Let $\kappa \cdot \beta$ be a closest corner of this square, i.e. an element in $\beta \cdot \mathbb{Z}[i]$ of smallest distance to α. Put $\rho = \alpha - \kappa\beta \in \mathbb{Z}[i]$. So $|\rho|$ is smaller or equal than half the diagonal of the square. So

$$\sqrt{\mathrm{N}(\rho)} = |\rho| \leqslant \frac{\sqrt{2}}{2} \cdot |\beta| < \sqrt{\mathrm{N}(\beta)}\,.$$

□

Definition. We say that α in $\mathbb{Z}[i]$ **divides** β in $\mathbb{Z}[i]$, denoted by $\alpha \mid \beta$ if there is a $\gamma \in \mathbb{Z}[i]$ such that $\beta = \gamma \cdot \alpha$.

Definition. An element $\delta \in \mathbb{Z}[i]$ is called a **a greatest common divisor** of α and β, if δ is an element in $\mathbb{Z}[i]$ of maximal norm such that $\delta \mid \alpha$ and $\delta \mid \beta$.

Note that if ε is a unit in $\mathbb{Z}[i]$ and δ a greatest common divisor of α and β then $\varepsilon \cdot \delta$ is also a greatest common divisor. A greatest common divisor can be computed with the Euclidian algorithm using the previous theorem. See the example below. The algorithm also yields two Gaussian integers ξ and η such that a chosen greatest common divisor δ can be written as $\delta = \xi\alpha + \eta\beta$. Conversely to the above, any two $\gcd(\alpha, \beta)$ are obtained by multiplying with a unit. See problem sheet.
Let $\alpha = 1 - 8\,i$ and $\beta = 5 + 5\,i$. So $\mathrm{N}(\alpha) = 65$ and $\mathrm{N}(\beta) = 50$. If $\kappa = -1 - i$, then $\rho = 1 + 2\,i$ with $\mathrm{N}(\rho) = 5 < \mathrm{N}(\beta)$.

$$\alpha = 1 - 8\,i = (-1 - i) \cdot \beta + (1 + 2\,i)\,.$$

In the next step we try to divide β by $\rho = 1 + 2\,i$. But actually β lies on the lattice $\rho\mathbb{Z}[i]$. We find

$$\beta = (3 - i) \cdot \rho + 0\,.$$

Hence $1 + 2i$ is a greatest common divisor of α and β.

Definition. An element $\pi \in \mathbb{Z}[i]$ is called a **Gaussian prime** if $\mathrm{N}(\pi) > 1$ and the following holds: if, for any α and $\beta \in \mathbb{Z}[i]$ such that π divides $\alpha \cdot \beta$, then π divides α or β.

Lemma 5.3. *Let $0 \neq \pi \in \mathbb{Z}[i]$. The following are equivalent*

- *π is a Gaussian prime*

- *If, for some α and $\beta \in \mathbb{Z}[i]$ we have $\pi = \alpha \cdot \beta$, then α or β is a unit.*

Proof. $\Downarrow$: If $\pi = \alpha \cdot \beta$, then $\pi \mid \alpha \cdot \beta$. Without loss of generality, we may assume that there is $\gamma \in \mathbb{Z}[i]$ such that $\alpha = \pi\gamma$. Then $\pi = \pi\gamma\beta$, so $\gamma\beta = 1$ shows that β is a unit and α is not a unit because π is not.
$\Uparrow$: Suppose π divides $\alpha \cdot \beta$. Let δ be a $\gcd(\alpha, \pi)$. So there is a γ such that $\pi = \gamma\delta$. By assumption, either δ or γ is a unit. If γ is a unit then $\pi\gamma^{-1} = \delta$ divides α. So π divides α. Otherwise δ is a unit. As $\delta = \xi\alpha + \eta\beta$ for some $\xi, \eta \in \mathbb{Z}[i]$, we get that π divides $\delta\beta$ and hence β. □

Lemma 5.4. *If $\pi \in \mathbb{Z}[i]$ is such that $\mathrm{N}(\pi)$ is a prime number then π is a Gaussian prime*

Proof. If $\pi = \alpha \cdot \beta$ then $\mathrm{N}(\alpha) \cdot \mathrm{N}(\beta) = \mathrm{N}(\pi)$. So either $\mathrm{N}(\alpha) = 1$ or $\mathrm{N}(\beta) = 1$. □

Example. $1 + i$ is a Gaussian prime of norm 2. Also $1 + 2\,i$ of norm 5 is a Gaussian prime. So $5 = (1 + 2\,i) \cdot (1 - 2\,i)$ is not a Gaussian prime. But $q = 3$ or $q = 7$ are Gaussian primes:

Lemma 5.5. *Let q be a prime number with $q \equiv 3 \pmod 4$. Then $q \in \mathbb{Z}[i]$ is a Gaussian prime.*

Proof. If $q = \alpha \cdot \beta$ for $\alpha = a + b\,i$ and $\beta \in \mathbb{Z}[i]$, then $q^2 = \mathrm{N}(q) = \mathrm{N}(\alpha) \cdot \mathrm{N}(\beta)$. But $\mathrm{N}(\alpha) = a^2 + b^2 = q \equiv 3 \pmod 4$ is not possible for $a, b \in \mathbb{Z}$. So either $\mathrm{N}(\alpha) = 1$ or $\mathrm{N}(\beta) = 1$. □

Lemma 5.6. *Let p be a prime number with $p \equiv 1 \pmod 4$. Then there exists a Gaussian prime π such that $p = \pi \cdot \overline{\pi}$.*

Proof. By quadratic reciprocity, $p \equiv 1 \pmod 4$ implies $(\frac{-1}{p}) = +1$. So there is a $c \in \mathbb{Z}$ such that $c^2 \equiv -1 \pmod p$. Hence p divides $(c - i)(c + i)$ in $\mathbb{Z}[i]$. But p does not divide $c + i$ or $c - i$. Therefore p is not a Gaussian prime. Hence there is $\alpha \cdot \beta$, both non-units, with $p = \alpha \cdot \beta$. By $p^2 = \mathrm{N}(p) = \mathrm{N}(\alpha) \cdot \mathrm{N}(\beta)$, we must have $\mathrm{N}(\alpha) = p$ and hence $\pi = \alpha$ is a Gaussian prime. And $p = \mathrm{N}(\pi) = \pi\overline{\pi}$. □

Proposition 5.7. *Up to associates, the Gaussian primes are the following :*

- *$1 + i$ is a Gaussian prime of norm 2.*
- *For each prime number $p \equiv 1 \pmod 4$ there are exactly two Gaussian primes π and $\overline{\pi}$ of norm p.*
- *Each prime number $q \equiv 3 \pmod 4$ is a Gaussian prime of norm q^2.*

Proof. All in the list are Gaussian primes. Let α be a Gaussian prime. Then there is a prime p dividing $\mathrm{N}(\alpha)$. In the above list we find a Gaussian prime π dividing p, so $\pi \mid p \mid \alpha\overline{\alpha}$. So either π or the Gaussian prime $\overline{\pi}$ divides α, and hence is associate to it. So α is in the above list. □

A **complete set of non-associate Gaussian primes** $\mathcal{P}_i$ is a set of Gaussian primes such that for each Gaussian prime π there is exactly one of the four associates in $\mathcal{P}_i$.

Theorem 5.8. *Let $\mathcal{P}_i$ be a complete set of non-associate Gaussian primes. Every $0 \neq \alpha \in \mathbb{Z}[i]$ can be written as*

$$\alpha = i^n \cdot \prod_{\pi \in \mathcal{P}_i} \pi^{a_\pi}$$

for some $0 \leqslant n < 4$ and $a_\pi \geqslant 0$. All but a finite number of a_π are zero and $a_\pi = \mathrm{ord}_\pi(\alpha)$ is the highest power of π dividing α.

Proof. Existence is proved by induction on $\mathrm{N}(\alpha)$. If $\mathrm{N}(\alpha) = 1$ then $\alpha = i^n$. If $\mathrm{N}(\alpha) > 1$, then there is a Gaussian prime π dividing α, so $\alpha = \pi\beta$ for some $\beta \in \mathbb{Z}[i]$. By induction hypothesis β has a factorisation, then so does α.
Suppose now α had two distinct factorisation of the above form

$$\alpha = i^n \cdot \prod_k \pi_k^{a_k} = i^{n'} \cdot \prod_j \pi_j^{b_j}$$

for some $0 \leqslant n, n' < 4$, $a_k \geqslant 0$ and $b_j \geqslant 0$. If a Gaussian prime from our set of non-associate Gaussian primes appears on both sides of this equation, we may divide by it. Therefore, we may assume that each Gaussian prime only appears on one side, i.e. $a_k \cdot b_k = 0$. Suppose there is still a Gaussian prime π_k dividing the left-hand side, i.e. $a_k > 0$ and $b_k = 0$. So π_k divides the right-hand side and hence divides one of its factors. It cannot divide $i^{n'}$ as π_k is not a unit. So it divides a $\pi_j^{b_j}$ with $b_j > 0$, so $k \neq j$. So it divides π_j, so there is a γ such that $\gamma \cdot \pi_k = \pi_j$. Since π_j is a Gaussian prime, either γ or π_k is a unit. Hence π_k and π_j are associate. Contradiction.
Hence, after this simplification each side is a power of i. So the factorisation of α is unique. □

Pythagorean triples

In this section we'll apply the arithmetic of $\mathbb{Z}[i]$ to solve a classical problem: finding all Pythagorean Triples.

Definition. A **Pythagorean triple** is a triple (x, y, z) where $x, y, z \in \mathbb{N}$ and $x^2 + y^2 = z^2$.

Examples: $3^2 + 4^2 = 5^2$ and $5^2 + 12^2 = 13^2$, so $(3, 4, 5)$ and $(5, 12, 13)$ are Pythagorean triples. How do we find all Pythagorean triples? Note that $x^2+y^2 = \mathrm{N}(x+iy)$, so Pythagorean triples come from Gaussian integers of square norm. The easiest way to get a Gaussian integer of square norm is to take the square of a Gaussian integer: $\alpha = (2 + i)^2 = 3 + 4i$ has norm $3^2 + 4^2 = (2^2 + 1^2)^2 = 5^2$, and $\beta = (3 + 2i)^2 = 5 + 12i$ has norm $5^2 + 12^2 = (3^2 + 2^2)^2 = 13^2$.
More generally, taking the norm of $\alpha = (a + bi)^2 = (a^2 - b^2) + 2abi$ gives

$$(a^2 - b^2)^2 + (2ab)^2 = (a^2 + b^2)^2,$$

so

$$(a^2 - b^2, 2ab, a^2 + b^2) \qquad \text{is a Pythagorean triple}$$

whenever $a > b > 0$. Our aim is to show that these are essentially all Pythagorean triples.
Note that if (x, y, z) is a Pythagorean triple then so is (kx, ky, kz) for all $k \geqslant 1$, so we may as well only look for **primitive Pythagorean triples** with $\gcd(x, y, z) = 1$, or equivalently $\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1$.
Secondly, in a primitive Pythagorean triple (x, y, z) we cannot have both x and y odd, since that would imply $z^2 = x^2 + y^2 \equiv 1 + 1 = 2 \pmod 4$ which is impossible. So we might as well assume that x is odd and y is even (interchanging x and y if necessary).

Theorem 5.9. *Let (x, y, z) be a primitive Pythagorean triple with y even. Then there exist coprime integers a, b with $a > b > 0$ and $a \not\equiv b \pmod 2$ such that*

$$x = a^2 - b^2, \qquad y = 2ab, \qquad z = a^2 + b^2.$$

Proof. Let $\alpha = x + y\,i \in \mathbb{Z}[i]$, so $\mathrm{N}(\alpha) = x^2 + y^2 = z^2$. The idea is to show that α is a square in $\mathbb{Z}[i]$; writing $\alpha = (a + b\,i)^2$ then gives the result.
We have

$$z^2 = \mathrm{N}(\alpha) = \alpha \cdot \overline{\alpha} = (x + y\,i)(x - y\,i).$$

We next show that the factors $x + y\,i$ and $x - y\,i$ are coprime in $\mathbb{Z}[i]$. If a Gaussian prime π divides both $x + y\,i$ and $x - y\,i$ then it divides $2x = (x + y\,i) + (x - i\,y)$ and also divides $2y\,i = (x + y\,i) - (x - i\,y)$; since x and y are coprime it then divides 2, so $\pi = 1 + i$ (times a unit). But $1 + i$ does *not* divide $x + y\,i$, since $x \not\equiv y \pmod 2$.
Hence $x + y\,i$ and $x - y\,i$ are coprime in $\mathbb{Z}[i]$. As their product is a square, unique factorisation in $\mathbb{Z}[i]$ implies that each is a square times a unit; using $-1 = i^2$, each must be either a square or i times a square.
Finally, $x + y\,i = (a + b\,i)^2$ leads to $x = a^2 - b^2$ and $y = 2ab$, while $x + y\,i = i(a + b\,i)^2$ leads to $x = -2ab$ and $y = a^2 - b^2$. Since $x, y > 0$ and x is odd we must be in the first case with $a > b > 0$, giving the result as stated. The conditions that $\gcd(a, b) = 1$ and $a \not\equiv b \pmod 2$ both follow from $\gcd(x, y) = 1$. □

Sums of two squares

In this lecture we will investigate the following related questions:

(i). For which $n \in \mathbb{N}$ can we solve $n = x^2 + y^2$ with $x, y \in \mathbb{Z}$?

(ii). Given $n \in \mathbb{N}$, how many solutions does the equation $n = x^2 + y^2$ have?

These questions can be rephrased in terms of Gaussian integers $\alpha = x + y\,i$, since $\mathrm{N}(\alpha) = \mathrm{N}(x + y\,i) = x^2 + y^2$:

(i). Which $n \in \mathbb{N}$ are norms of Gaussian integers $\alpha \in \mathbb{Z}[i]$?

(ii). Given $n \in \mathbb{N}$, how many Gaussian integers $\alpha \in \mathbb{Z}[i]$ have norm n?

Lemma 5.10. *Any prime $p \equiv 1 \pmod 4$ can be written as a sum of two squares.*

Proof. By lemma 5.6 we have $p = \pi\overline{\pi}$ for some Gaussian prime $\pi = x + y\,i$. Then $p = x^2 + y^2$. □

Theorem 5.11. *Let $n = a \cdot b^2$ be an integer with a square-free. Then n can be written as a sum of two squares if and only if no prime $q \equiv 3 \pmod 4$ divides a.*

Proof. $\Leftarrow$: For every prime p dividing a, there is a Gaussian prime π_p of norm p by Proposition 5.7. Put $x + iy = b \cdot \prod_{p|a} \pi_p$. Then $x^2 + y^2 = n$.
$\Rightarrow$: Let $n = x^2 + y^2 = (x + i\,y)(x - i\,y)$. If a prime $q \equiv 3 \pmod 4$ divides n then, as it is a Gaussian prime by Lemma 5.5, it divides $x + i\,y$ or $x - i\,y$. So q divides x and y, hence q^2 divides n. The statement can now be proved by induction on b. □

We will use L-functions to solve the second question, making further use of the Dirichlet character χ_1 introduced in Chapter 4:

$$\chi_1(n) = \begin{cases} +1 & \text{if } n \equiv 1 \pmod 4; \\ -1 & \text{if } n \equiv 3 \pmod 4; \\ 0 & \text{if } n \text{ is even.} \end{cases}$$

The connection with $\mathbb{Z}[i]$ can be seen if we recall how ordinary prime numbers p factorise in $\mathbb{Z}[i]$, which depends on p modulo 4.

Theorem 5.12. *For each $n \in \mathbb{N}$, the number of integral solutions x, y to the equation $n = x^2 + y^2$ is given by $4\sum_{d|n} \chi_1(d)$. The number of solutions with $x > 0$ and $y \geqslant 0$ is $\sum_{d|n} \chi_1(d)$.*

Remark. To each solution (x, y) corresponding to $\alpha = x + y\,i \in \mathbb{Z}[i]$, we find three more corresponding to the associates $i\alpha$, $-\alpha$ and $-i\alpha$, namely $(-y, x)$, $(-x, -y)$, $(y, -x)$. Also, if $x \neq y$ then there are four more solutions coming from $\overline{\alpha}$ and its associates, obtained by interchanging x and y.

Examples: If n is 9, then $\sum_{d|9} \chi_1(d) = \chi_1(1) + \chi_1(3) + \chi_1(9) = 1 - 1 + 1 = 1$, and the single solution with $x > 0$ and $y \geqslant 0$ is $(x, y) = (3, 0)$.
If $n = 25$, then $\sum_{d|25} \chi(d) = \chi_1(1) + \chi_1(5) + \chi_1(25) = 1 + 1 + 1 = 3$, and solutions are $(x, y) = (3, 4)$, $(4, 3)$, $(5, 0)$.
Suppose now that $n = p$ is a prime number. Then $\sum_{d|p} \chi_1(d) = \chi_1(1) + \chi_1(p) = 1 + \chi_1(p)$, which equals 1 when $p = 2$ (solution: $(1, 1)$); equals 0 when $p \equiv 3 \pmod 4$ (no solutions); and equals 2 when $p \equiv 1 \pmod 4$ (two solutions, differing only in the order of x and y, for example $61 = 5^2 + 6^2 = 6^2 + 5^2$ only).

Example. Find all ways of writing $n = 130$ as a sum of two squares.

Proof of Theorem 5.12. Let a_n be the number of solutions to $n = x^2 + y^2$ with $x, y \in \mathbb{Z}$, which is the number of elements $\alpha = x + y\,i \in \mathbb{Z}[i]$ with norm n. Then

$$\sum_{n \geqslant 1} \frac{a_n}{n^s} = \sum_{0 \neq \alpha \in \mathbb{Z}[i]} \frac{1}{\mathrm{N}(\alpha)^s}.$$

By unique factorisation in $\mathbb{Z}[i]$, the latter sum has an Euler product expansion:

$$\sum_{0 \neq \alpha \in \mathbb{Z}[i]} \frac{1}{\mathrm{N}(\alpha)^s} = 4 \prod_{\pi \in \mathcal{P}_i} \frac{1}{1 - \mathrm{N}(\pi)^{-s}},$$

where the product is over all prime elements π of $\mathbb{Z}[i]$, choosing one from each set of four associate primes, and the factor of 4 allows for the unit factor in the factorisation of each α. Now we look at the factors for each type of Gaussian prime in turn:

(i). $\pi = 1 + i$ with $\mathrm{N}(\pi) = 2$ contributes a factor $1/(1 - 2^{-s})$.

(ii). each π with $\mathrm{N}(\pi) = p \equiv 1 \pmod 4$ contributes a factor $1/(1 - p^{-s})$, and there are two such Gaussian primes for each prime $p \equiv 1 \pmod 4$.

(iii). each $\pi = q \equiv 3 \pmod 4$ with $\mathrm{N}(\pi) = q^2$ contributes a factor of $1/(1 - q^{-2s})$.

Hence our product is

$$\prod_{\pi \in \mathcal{P}_i} \frac{1}{1 - \mathrm{N}(\pi)^{-s}} = \left(\frac{1}{1 - 2^{-s}}\right) \left(\prod_{p \equiv 1 \bmod 4} \frac{1}{(1 - p^{-s})^2}\right) \left(\prod_{q \equiv 3 \bmod 4} \frac{1}{1 - q^{-2s}}\right) = \zeta(s) \cdot L(s, \chi_1)$$

using an exercise from problem sheet 4 at the end. So we have

$$\frac{1}{4}\sum_{n\geqslant 1}\frac{a_n}{n^s} = \zeta(s)\cdot L(s,\chi_1) = \left(\sum_{m\geqslant 1}\frac{1}{m^s}\right)\left(\sum_{d\geqslant 1}\frac{\chi(d)}{d^s}\right).$$

Comparing coefficients:

$$\frac{1}{4}a_n = \sum_{md=n}\chi_1(d) = \sum_{d|n}\chi_1(d).$$

□

Remark. The function

$$\zeta(s,\mathbb{Z}[i]) = \frac{1}{4}\sum_{0\neq\alpha\in\mathbb{Z}[i]}\frac{1}{\mathrm{N}(\alpha)^s}$$

is the zeta function of $\mathbb{Z}[i]$; it is analogous to the Riemann zeta function

$$\zeta(s) = \frac{1}{2}\sum_{0\neq n\in\mathbb{Z}}\frac{1}{|n|^s}.$$

Remark. Since $a_n \geqslant 0$, the formula we proved has the consequence that for each $n\in\mathbb{N}$, the number of divisors of n which are congruent to 1 modulo 4 is greater or equal the number of divisors which are congruent to 3 modulo 4.

Sums of more squares

In the previous section, we found a formula for the number of integral solutions to $n = x^2+y^2$ for any given $n\in\mathbb{N}$. In particular this equation has a solution whenever $n = p \equiv 1 \pmod 4$. Now we know that not every integer is a sum of two squares, can we do any better by taking sums of *three* squares? Now $3 = 1^2+1^2+1^2$ and $6 = 1^2+1^2+2^2$, but 7 is not a sum of three squares. In fact, no integer $n\equiv 7 \pmod 8$ is a sum of three squares, since all squares are congruent to 0, 1 or 4 modulo 8.
Instead of answering the question "exactly which positive integers are sums of three squares" (which turns out to be quite difficult) we'll move on to four squares, where there is a classical result.

Theorem 5.13 (Lagrange, 1770). *Every positive integer is a sum of four squares.*

In other words, for every $n\in\mathbb{N}$ there exist $x,y,z,w\in\mathbb{Z}$ (including zero) such that $n = x^2+y^2+z^2+w^2$.

Theorem 5.14 (Jacobi). *Let $n\geqslant 1$ be an integer. Let A_n be the number of solutions $x,y,z,w\in\mathbb{Z}$ to the equation $x^2+y^2+z^2+w^2 = n$. Then*

$$A_n = \begin{cases} 8\sum_{d|n} d & \text{if } n \text{ is odd and} \\ 24\sum_{2\nmid d|n} d & \text{if } n \text{ is even.}\end{cases}$$