MAU22103/33101 - Introduction to Number Theory

Exercise Sheet 5

Trinity College Dublin

Course homepage

Answers are due for Friday November 22nd, 2pm.
The use of electronic calculators and computer algebra software is allowed.

Exercise 1 *A yearly exercise*

In the following, you may freely use the results of Exercises 6 and 8 to determine irreducibles of prime norm $p \equiv 1 \pmod 4$, though it is probably less efficient than trial and error for primes under 500.

1. (30 pts) Determine a factorisation into irreducibles of $20 + 24i$.
2. (30 pts) Determine a factorisation into irreducibles of $20 + 48i$.
3. (40 pts) Determine non-zero $a, b \in \mathbb{Z}$ such that

$$6066 = a^2 + b^2.$$

Solution 1

1. We first note that that

$$20 + 24i = 4(5 + 6i).$$

Since $\mathrm{N}(5 + 6i) = 25 + 36 = 61$, which is prime, $(5 + 6i)$ is irreducible. Hence, it suffices to factorise

$$4 = 2^2 = (1 + i)^2(1 - i)^2 = (-i)^2(1 + i)^4 = -(1 + i)^4.$$

Hence, a factorisation into irreducibles of $20 + 24i$ is

$$20 + 24i = -(1 + i)^4(5 + 6i).$$

Some other possible factorisations are given below for comparison

$$20+24i = -(1-i)^4(5+6i) = -i(1+i)^4(6-5i) = -i(1-i)^4(6-5i) = i(1+i)^4(-6+5i)$$

2. We first note that

$$20 + 48i = 4(5 + 12i) = -(1 + i)^4(5 + 12i)$$

and we just have to factorise $5 + 12i$. This has norm $5^2 + 12^2 = 169 = 13^2$, and so

$$5 + 12i = \nu\pi_{13,1}\pi_{13,2}$$

for some irreducibles $\pi_{13,1}$, $\pi_{13,2}$ of norm 13, and a unit ν. A pair of non-associate irreducibles of norm 13 are given by $2 \pm 3i$ (these are irreducible as they have prime norm). Up to changing ν, we can therefore assume

$$\pi_{13,1},\ \pi_{13,2} \in \{2 + 3i,\ 2 - 3i\}.$$

If $\pi_{13,1} \neq \pi_{13,2}$, then $\pi_{13,1}\pi_{13,2} = 13$ divides $5 + 12i$, which is clearly impossible. Hence $\pi_{13,1} = \pi_{13,2}$. We can quickly check that

$$(2 + 3i)^2 = -5 + 12i \text{ and } (2 - 3i)^2 = -5 - 12i$$

the latter of which is associate to $5 + 12i$. Thus

$$5 + 12i = -(2 - 3i)^2$$

and hence

$$20 + 48i = (1 + i)^4(2 - 3i)^2$$

is a factorisation into irreducibles. Some alternative factorisations are given below

$$20 + 48i = (1 - i)^4(2 - 3i)^2 = -(1 + i)^4(3 + 2i)^2$$

3. We can factorise $6066 = 2 \times 9 \times 337$ into powers of primes. We have that

   $$2 = \mathrm{N}(1 + i) \text{ and } 9 = \mathrm{N}(3).$$

   Thus, if we can write 337 as a norm, we are essentially done.

   Given that 337 is relatively small, applying either of the Exercises mentioned seems like overkill, when we can quite quickly check all small squares by hand. The squares less than or equal to 337 are

   0, 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, 256, 289, 324.

   This leads us to

   $$337 = 81 + 256 = 9^2 + 16^2 = \mathrm{N}(9 + 16i).$$

   Hence

   $$6066 = \mathrm{N}(3 \times (1 + i) \times (9 + 16i)) = \mathrm{N}(-21 + 75i) = 21^2 + 75^2$$

This was the only exercise that you must submit before the deadline. The following exercises are not mandatory; they are not worth any points, and you do not have to submit them

However, I strongly encourage you to give them a try, as the best way to learn number theory is through practice.

The exercises marked with a star are the exercises I will try to talk about in the tutorial lecture. If there are any exercises would would particularly like to discuss, please let me know

The exercises are arranged by theme, and roughly in order of difficulty within each theme, with the first few working as good warm-ups, and the remainder being of similar difficulty to the main exercise. You are welcome to email me if you have any questions about them. The solutions will be made available with the solution to the main exercise.

Exercise 2 *Division with remainder* ★

For the given α, $\beta \in \mathbb{Z}[i]$, determine γ, $\rho \in \mathbb{Z}[i]$ such that

$$\alpha = \beta\gamma + \rho \text{ and } \mathrm{N}(\rho) < \mathrm{N}(\beta).$$

i) $\alpha = 8 + 5i$, $\beta = 2 + 3i$,

ii) $\alpha = 15 + 2i$, $\beta = 4 - i$,

iii) $\alpha = 12 + 37i$, $\beta = 7 + 9i$

iv) $\alpha = 19 + 93i$, $\beta = 4 + 5i$.

Solution 2

i) We have that

$$\frac{\alpha}{\beta} = \frac{8+5i}{2+3i} = \frac{(8+5i)(2-3i)}{13} = \frac{31}{13} + \frac{-14i}{13} \approx 2 - i.$$

Letting $\gamma = 2 - i$, we define

$$\rho = \alpha - \beta\gamma = 8 + 5i - (2+3i)(2-i) = 8 - 7 + 5i - 4i = 1 + i$$

which has norm $2 < 13$.

ii) We compute

$$\frac{\alpha}{\beta} = \frac{15+2i}{4-i} = \frac{58+23i}{17} \approx 3 + i.$$

Letting $\gamma = 3 + i$, we define

$$\rho = \alpha - \beta\gamma = 15 + 2i - 13 - i = 2 + i$$

which has norm $5 < 17$.

iii) We compute

$$\frac{\alpha}{\beta} = \frac{12+37i}{7+9i} = \frac{417+151i}{130} \approx 3 + i$$

Letting $\gamma = 3 + i$, we define

$$\rho = \alpha - \beta\gamma = 12 + 37i - 12 - 34i = 3i$$

which has norm $9 < 130$.

iv) We compute

$$\frac{\alpha}{\beta} = \frac{19+93i}{4+5i} = \frac{541+277i}{41} \approx 13+7i$$

Letting $\gamma = 13+7i$, we define

$$\rho = \alpha - \beta\gamma = 19 + 93i - 17 - 93i = 2$$

which has norm $4 < 41$.

Exercise 3 *Relative division*

Let $a, b \in \mathbb{Z}$. We can consider these both as (classical) integers and as Gaussian integers. We write $a|_{\mathbb{Z}}b$ if a divides b when viewed as integers, and $a|_{\mathbb{Z}[i]}b$ when a divides b when viewed as Gaussian integers.

Show that $a|_{\mathbb{Z}}b$ if and only if $a|_{\mathbb{Z}[i]}b$.

Solution 3

If $a|_{\mathbb{Z}}b$, there exists $c \in \mathbb{Z} \subset \mathbb{Z}[i]$ such that $b = ac$, so $a|_{\mathbb{Z}[i]}b$. Conversely, suppose there exists $\gamma \in \mathbb{Z}[i]$ such that $b = a\gamma$. Letting $\gamma = c + di$, we have that

$$b = ac + adi$$

and hence $ad = 0$. If $a = 0$, then $b = 0$, and so $a|_{\mathbb{Z}}b$. If $a \neq 0$, then $d = 0$, and so $b = ac$, which means that $a|_{\mathbb{Z}}b$.

Exercise 4 *Bezout's Theorem*

For the given α, $\beta \in \mathbb{Z}[i]$, determine η, $\xi \in \mathbb{Z}[i]$ such that $\alpha\xi + \beta\eta$ is a greatest common divisor of α and β.

i) $\alpha = 6 + 2i$, $\beta = 4 + 3i$,

ii) $\alpha = 4 + 6i$, $\beta = 5 + 3i$.

Solution 4

i) We apply Euclid's algorithm:

$$\begin{aligned}
\frac{6+2i}{4+3i} &= \frac{30-10i}{25} \approx 1,\\
6+2i &= 4+3i+(2-i),\\
\frac{4+3i}{2-i} &= \frac{5+10i}{5} = 1+2i.
\end{aligned}$$

Hence, $\gcd(6+2i, 4+3i) = 2-i$ and

$$2-i = 6+2i-(4+3i).$$

ii) We apply Euclid's algorithm:

$$\begin{aligned}
\frac{4+6i}{5+3i} &= \frac{38+18i}{34} \approx 1+i,\\
4+6i &= (1+i)(5+3i)+(2-2i),\\
\frac{5+3i}{2-2i} &= \frac{4+16i}{8} \approx 2i,\\
5+3i &= 2i(2-2i)+(1-i),\\
2-2i &= 2(1-i).
\end{aligned}$$

Hence, $\gcd(4+6i, 5+3i) = 1-i$ and

$$\begin{aligned}
1-i = 5+3i-2i(2-2i)&\\
5+3i-2i(4+6i-(1+i)(5+3i))&\\
= -2i(4+6i)+(1+2i-2)(5+3i)&\\
= -2i(4+6i)+(-1+2i)(5+3i).&
\end{aligned}$$

Exercise 5 *Complete factorisation* ★

Determine a complete factorisation into irreducibles of the following $\alpha \in \mathbb{Z}[i]$.

i) $\alpha = 5+3i$,

ii) $\alpha = 8-i$,

iii) $\alpha = 13+9i$,

iv) $\alpha = 19+12i$.

Solution 5

i) The norm of *alpha* is $\mathrm{N}(\alpha) = 25 + 9 = 34 = 2 \times 17$. Hence

$$\alpha = \nu\pi_2\pi_{17}$$

for irreducibles of norms 2 and 17, respectively. Up to a unit, $\pi_{17} = 1 \pm 4i$ and so we must test divisibility:

$$\frac{5+3i}{1+4i} = \frac{17-17i}{17} = (1-i)$$

and so

$$5 + 3i = (1-i)(1+4i)$$

is a factorisation into irreducibles.

ii) We compute $\mathrm{N}(\alpha) = 65 = 5 \times 13$. Hence

$$\alpha = \nu\pi_5\pi_{13}$$

for some irreducibles of norms 5 and 13. If we can determine which of the two non-associate irreducibles $2 + i$ or $2 - i$, of norm 5, divides α, we are essentially done.

We check that

$$\frac{8-i}{2+i} = \frac{15-10i}{5} = 3 - 2i$$

and hence

$$8 - i = (2+i)(3-2i)$$

is a factorisation into irreducibles.

iii) $\mathrm{N}(\alpha) = 250 = 2 \times 5^3$. Thus

$$\alpha = \nu\pi_2\pi_{5,1}\pi_{5,2}\pi_{5,3}$$

for a unit ν, and irreducibles of norms 2 and 5. Since $5 \nmid 13 + 9i$, we must have have that all the irreducibles of norm 5 are equal. We can check

$$\frac{13+9i}{2+i} = \frac{35+5i}{5} = 7 + i$$

and so we can take $\pi_{5,1} = \pi_{5,2} = \pi_{5,3} = 2 + i$. We can take $\pi_2 = 1 + i$, and so it remains to determine ν:

$$\nu = \frac{13 + 9i}{(1 + i)(2 + i)^3} = \frac{13 + 9i}{-9 + 13i} = -i.$$

Thus

$$13 + 9i = -i(1 + i)(2 + i)^3.$$

We could also have absorbed the unit into π_2 by determining

$$\pi_2 = \frac{13 + 9i}{(2 + i)^3} = \frac{13 + 9i}{2 + 11i} = 1 - i$$

giving an alternative factorisation

$$13 + 9i = (1 - i)(2 + i)^3.$$

iv) $\mathrm{N}(\alpha) = 505 = 5 \times 101$. Let us check if α is divisible by the irreducible $2 + i$:

$$\frac{19 + 12i}{2 + i} = \frac{50 + 5i}{5} = 10 + i$$

and hence

$$19 + 12i = (2 + i)(10 + i)$$

is a factorisation into irreducibles.

Exercise 6 *An answer to your prayers* ★

Let p be a prime number such that $p \equiv 1 \pmod 4$. We will give a partial algorithm, the Hermite-Serret algorithm, to determine $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$.

i) Show that there exists $c \in \mathbb{Z}$ such that $c^2 + 1 \equiv 0 \pmod p$.

ii) Let $\pi \in \mathbb{Z}[i]$ be an irreducible of norm p. Show that either π or $\overline{\pi}$ divides $c + i$.

iii) Hence conclude that if $a + bi \sim \gcd(p, c + i)$, then $a^2 + b^2 = p$.

For odd p, we showed that $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$ for every integer a. As such, given $a \in \mathbb{Z}$ such that $a^{\frac{p-1}{2}} \equiv -1 \pmod p$, for $p \equiv 1 \pmod 4$, $c \equiv a^{\frac{p-1}{4}}$ gives us the input we need for this algorithm. Picking a at random, we have a 1-in-2 change of finding such an a. This gives a remarkably efficient algorithm, at least when implemented by a computer rather than a human.

Solution 6

i) Since $p \equiv 1 \pmod 4$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$. As such, there exists $c \in \mathbb{Z}$ such that $c^2 \equiv -1 \pmod p$, and so
$$c^2 + 1 \equiv 0 \pmod p$$

ii) We know that $p|c^2+1$, and $p = \pi\overline{\pi}$ where both π and $\overline{\pi}$ are irreducible. Hence
$$\pi|c^2+1 = (c+i)(c-i) \text{ and } \overline{\pi}|c^2+1 = (c+i)(c-i).$$
As π and $\overline{\pi}$ are irreducible, this means that
$$\pi|c+i \text{ or } \pi|c-i \text{ and } \overline{\pi}|c+i \text{ or } \overline{p}|c-i.$$
If both π and $\overline{\pi}$ divide the same factor, then $\pi\overline{\pi} = p$ divides it, and so one of $\frac{c}{p} + \frac{i}{p}$ or $\frac{c}{p} - \frac{i}{p}$ is a Gaussian integer. This is impossible, and so either
$$\pi|c+i \text{ and } \overline{\pi}|c-i$$
or
$$\pi|c-i \text{ and } \overline{\pi}|c+i$$
as needed.

iii) As $p = \pi\overline{\pi}$ is a factorisation into irreducibles, the divisors of p are (associate to) 1, π, $\overline{\pi}$ and p. In particular, $\gcd(p, c+i)$ is one of 1, π, $\overline{\pi}$ or p. As p does not divide $c+i$, and one of π or $\overline{\pi}$ does divide $c+i$, we must have that
$$\gcd(p, c+i) = \pi \text{ or } \gcd(p, c+i) = \overline{\pi}$$
up to multiplication by a unit. In either case, $\gcd(p, c+i)$ is an irreducible of norm p. In particular, if $a+bi$ is a $\gcd(p, c+i)$, then $a^2+b^2 = p$.

Exercise 7 *An application of your prayers* ★

For each of the following primes p, use the results of Exercise 6 to determine $a, b \in \mathbb{Z}$ such that $a^2 + b^2 = p$.

i) $p = 13$.

ii) $p = 29$.

iii) $p = 61$.

iv) $p = 337$. Note that $189^2 \equiv -1 \pmod{337}$.

v) $p = 1993$. Note that $834^2 \equiv -1 \pmod{1993}$

Solution 7

i) We need to find a square root of -1 modulo 13. The easiest option is to note that $5^2 = 25 = 2(13) - 1$, and so 5 works. Thus, it suffices to compute $\gcd(13, 5 + i)$. We will perform Euclid's algorithm:

$$\begin{aligned}\frac{13}{5+i} &= \frac{65-13i}{26} \approx 3, \\ 13 &= (5+i)(3) + (-2-3i), \\ \frac{5+i}{-2-3i} &= \frac{-13+13i}{13} = -1+i,\end{aligned}$$

and hence $-2 - 3i$ is a gcd. Thus $13 = 2^2 + 3^2$.

ii) We need to find a square root of -1 modulo 29. As described below Exercise 6, we will try to find a such that $a^{14} \equiv -1 \pmod{29}$. Let us try $a = 2$:

$$2^{14} \equiv 16 \times 32^2 \equiv 16 \times 9 \equiv 19 \times 3 \equiv 57 \equiv -1 \pmod{29}$$

and so $c \equiv 2^7 \equiv 32 \times 4 \equiv 12 \pmod{29}$ gives us a choice of square root of -1.

Now we must compute $\gcd(29, 12 + i)$:

$$\begin{aligned}\frac{29}{12+i} &= \frac{348-29i}{145} \approx 2, \\ 29 &= (12+i)(2) + 5 - 2i, \\ \frac{12+i}{5-2i} = \frac{58+29i}{29} &= 2+i,\end{aligned}$$

and hence $29 = 2^2 + 5^2$.

iii) We need to find a square root of -1 modulo 61. It suffices to find a such that $a^{30} \equiv -1 \pmod{61}$. We will try $a = 2$:

$$2^{30} \equiv (2^6)^5 \equiv 3^5 \equiv 3 \times 20 \equiv -1 \pmod{61}$$

and so we can take c given by

$$2^{15} \equiv 8 \times 3^2 \equiv 72 \equiv 11 \pmod{61}.$$

So, it suffices to compute $\gcd(61, 11 + i)$:

$$\begin{aligned} \frac{61}{11+i} &= \frac{671 - 11i}{122} \approx 6, \\ 61 &= (11+i)(6) + (-5 - 6i) \end{aligned}$$

and we can stop there, noting that $61 = 5^2 + 6^2$.

iv) We are given a square root of -1, so it suffices to compute $\gcd(337, 189 + i)$:

$$\begin{aligned} \frac{337}{189+i} &= \frac{63693 - 337i}{35722} \approx 2, \\ 337 &= (189+i)(2) + (-41 - 2i), \\ \frac{189+i}{41+2i} &= \frac{7751 - 337i}{1685} \approx 5, \\ 189 + i &= (41 + 2i)(5) + (-16 - 9i) \end{aligned}$$

and we can stop there, as $337 = 9^2 + 16^2$.

v) We are given a square root of -1, so it suffices to compute $\gcd(1993, 834 + i)$:

$$\begin{aligned} \frac{1993}{834+i} &= \frac{1662162 - 834i}{714026} \approx 2, \\ 1993 &= (834+i)(2) + (325 - 2i), \\ \frac{834+i}{325-2i} &= \frac{271056 - 1993i}{105625} \approx 3, \\ 834 + i &= (325 - 2i)(3) + (-141 + 7i), \\ 325 - 2i &= (141 - 7i)(2) + (43 + 12i) \end{aligned}$$

and we can stop there, as $1993 = 12^2 + 43^2$.

Exercise 8 *Gauss on high*

Let $p = 4k + 1$. Gauss showed that the integers a, b determined by

$$-\frac{p}{2} \leq a, b \leq \frac{p}{2}$$

and

$$a \equiv \frac{(2k)!}{2(k!)^2} \pmod{p} \text{ and } b \equiv a(2k)! \pmod{p}$$

satisfy $a^2 + b^2 = p$. We will give a partial proof of this.

i) Show that, for all $k \geq 1$, $\frac{(2k)!}{2(k!)^2} \in \mathbb{Z}$.

Hint: What does $\frac{(2k)!}{(k!)^2}$ count? Why would this be even?

ii) Show that

$$(2k)! \equiv (-1)^{2k}(4k)(4k-1)(\cdots)(2k+1) \pmod{4k+1}$$

iii) Hence, show that $(2k)!^2 \equiv -1 \pmod{4k+1}$

Hint: Recall Wilson's theorem from an earlier exercise set. This says that $(p-1)! \equiv -1 \pmod{p}$.

iv) Hence conclude that

$$a^2 + b^2 \equiv 0 \pmod{p}$$

if

$$a \equiv \frac{(2k)!}{2(k!)^2} \pmod{p} \text{ and } b \equiv a(2k)! \pmod{p}$$

Solution 8

i) The ratio $\frac{(2k)!}{(k!)^2}$ is the binomial coefficient $\binom{2k}{k}$, which counts the number of ways of choosing k elements from a set of $2k$. If X is a set of $2k > 0$ elements, the subsets of X containing k elements, come in pairs $(A, X \setminus A)$, and hence there are an even number of such subsets. Thus $\frac{1}{2}\binom{2k}{k}$ is an integer.

ii) For each $1 \leq r \leq 2k$, $4k+1-r \equiv -r \pmod{4k+1}$, and hence

$$\begin{aligned}(-1)^{2k}(4k)(4k-1)(\cdots)(2k+1) &\equiv \prod_{r=1}^{2k} -(4k+1-r)\\ &\equiv \prod_{r=1}^{2k} r \equiv (2k)! \pmod{4k+1}\end{aligned}$$

iii) We have that

$$(2k)!^2 \equiv (2k)! \times (-1)^{2k}(4k)(4k-1)\cdots(2k+1) \equiv (4k)! \equiv -1 \pmod{4k+1}$$

by Wilson's theorem.

iv) For a and b as given

$$a^2+b^2 \equiv \frac{(2k)!^2}{4(k!)^4} + \frac{(2k)!^4}{4(k!)^4} \equiv \frac{-1}{4(k!)^4} + \frac{1}{4(k!)^4} \equiv 0 \pmod{4k+1}$$

as needed.

Exercise 9 *Forcing a common factor*

Let α, $\beta \in \mathbb{Z}[i]$, and let $\gcd(\alpha,\beta)$ be a greatest common divisor of α and β.

i) Show that $\mathrm{N}(\gcd(\alpha,\beta)) \,|\, \gcd(\mathrm{N}(\alpha),\mathrm{N}(\beta))$.

ii) Give an example of α, β such that

$$\mathrm{N}(\gcd(\alpha,\beta)) < \gcd(\mathrm{N}(\alpha),\mathrm{N}(\beta)).$$

iii) Suppose that $\gcd(\mathrm{N}(\alpha),\mathrm{N}(\beta)) = p$ is prime. Show that $p \not\equiv -1 \pmod 4$.

iv) Suppose that $\gcd(\mathrm{N}(\alpha),\mathrm{N}(\beta)) = p$. Show that at least one of

$$\gcd(\alpha,\beta) \text{ or } \gcd(\alpha,\overline{\beta})$$

is not a unit.

v) Suppose that $\gcd(\mathrm{N}(\alpha),\mathrm{N}(\beta)) = n > 1$. Show that at least one of

$$\gcd(\alpha,\beta) \text{ or } \gcd(\alpha,\overline{\beta})$$

is not a unit.

Solution 9

i) We know $\gcd(\alpha, \beta)|\alpha$ and hence

$$\mathrm{N}(\gcd(\alpha, \beta))|\,\mathrm{N}(\alpha),$$

and similarly

$$\mathrm{N}(\gcd(\alpha, \beta))|\,\mathrm{N}(\beta).$$

Hence

$$\mathrm{N}(\gcd(\alpha, \beta))|\,\gcd(\mathrm{N}(\alpha), \mathrm{N}(\beta)).$$

ii) If we can find α and β that are coprime, with the same norm, we are done. For example $2 + i$ and $2 - i$ are coprime: they are irreducible and non associate, so much be coprime. Thus

$$\mathrm{N}(\gcd(2 + i, 2 - i)) = 1 < 5 = \gcd(\mathrm{N}(2 + i), \mathrm{N}(2 - i))$$

as needed.

iii) Recall that if $p \equiv -1 \pmod 4$, p is irreducible and hence $p|\,\mathrm{N}(\alpha)$ implies that $p|\alpha$, and hence $\mathrm{N}(p) = p^2|\,\mathrm{N}(\alpha)$. Similarly for β. Thus,

$$p^2|\,\gcd(\mathrm{N}(\alpha), \mathrm{N}(\beta)) = p$$

which is a contradiction. Thus, we must have $p \not\equiv -1 \pmod 4$.

iv) Let $p = \pi_p\overline{\pi}_p$ be a factorisation of p into irreducibles. If $p|\,\mathrm{N}(\gamma)$ then γ is divisible by one of π_p or $\overline{\pi}_p$. In particular, if

$$p|\,\gcd(\mathrm{N}(\alpha), \mathrm{N}(\beta))$$

we must have that, swapping π_p and $\overline{\pi}_p$ if necessary, $\pi_p|\alpha$ and one of π_p or $\overline{\pi}_p$ divides β. If $\pi_p|\beta$, then $\pi_p|\,\gcd(\alpha, \beta)$, and so $\gcd(\alpha, \beta)$ is not a unit. If $\overline{\pi}_p|\beta$, then $\pi_p|\overline{\beta}$. Hence $\pi_p|\,\gcd(\alpha, \overline{\beta})$, and so $\gcd(\alpha, \overline{\beta})$ is not a unit.

v) We did not use anything about $\gcd(\mathrm{N}(\alpha), \mathrm{N}(\beta))$ other than being divisible by a prime number not congruent to $-1 \pmod 4$ in the previous argument. Thus the same argument applies if such a prime divisor exists. If a prime divisor $p \equiv -1 \pmod 4$ exists, then, as in part (iii), $p|\alpha$ and $p|\beta$ and so $p|\,\gcd(\alpha, \beta)$, and so it is not a unit.

Exercise 10 *Number of representations*

Given $n \in \mathbb{N}$, how many ordered pairs of integers (r, s) are there such that $r^2 + s^2 = n$? Ordered here means we consider (r, s) as distinct from (s, r).

i) Show that every (r, s) such that $r^2+s^2 = n$ are in bijection with $\alpha \in \mathbb{Z}[i]$ such that $\mathrm{N}(\alpha) = n$

ii) Fix an irreducible π_p for each prime p and let

$$n = 2^a \prod_{p\equiv 1 \pmod 4} p^{b_p} \prod_{q\equiv -1 \pmod 4} q^{c_q}.$$

Describe the factorisation into irreducibles of $\alpha \in \mathbb{Z}[i]$ such that $\mathrm{N}(\alpha) = n$.

iii) Hence, determine the number of ordered pairs of integers (r, s) are there such that $r^2 + s^2 = n$, in terms of a, b_p, c_q.

Solution 10

i) It is quite clear that the map $(r, s) \mapsto r + si$ gives the decided bijection.

ii) If c_q is not even for some prime $q \equiv -1 \pmod 4$, then so such α exists. Otherwise, every such α can be written as

$$\alpha = \nu(1 + i)^a \prod_{p\equiv 1 \pmod p} \pi_p^{d_p} \overline{\pi}_p^{e_p} \prod_{q\equiv -1 \pmod p} q^{\frac{c_q}{2}}$$

for some unit ν, and integers d_p, $e_p \geq 0$ such that $d_p + e_p = b_p$.

iii) The number of such ordered pairs is equal to the number of Gaussian integers of norm n. There are no such Gaussian integers if c_q is odd for any prime $q \equiv -1 \pmod 4$. If c_q is even for every prime $q \equiv -1 \pmod 4$, then every such Gaussian integer is determined uniquely by a choice of unit ν (4 possibilities), and integers $d_p, e_p \geq 0$ such that $d_p + e_p = b_p$ ($b_p + 1$ possibilities) for each prime $p \equiv 1 \pmod 4$. Hence, the number of such ordered pairs is

$$\begin{cases} 0 \text{ if } c_q \equiv 1 \pmod 2 \text{ for some prime } q \equiv -1 \pmod 4, \\ 4 \prod_{\substack{p \mid n \\ p\equiv 1 \pmod 4}} (b_p + 1) \text{ otherwise} \end{cases}$$

Exercise 11 *A Euclidean failure*

Define a subspace of $\mathbb{C}$ by

$$\mathbb{Z}[\sqrt{-3}] := \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$$

i) Show that $\mathbb{Z}[\sqrt{-3}]$ is a ring: it is closed under addition and multiplication. Define what it means for $\alpha \in \mathbb{Z}[\sqrt{-3}]$ to divide $\beta \in \mathbb{Z}[\sqrt{-3}]$ in this ring.

ii) Define the norm of $\alpha = a + b\sqrt{-3}$ by

$$\mathrm{N}(\alpha) = \alpha\overline{\alpha} = a^2 + 3b^2$$

Show that the only elements of norm 1 are ±1.

iii) Suppose that given α, $\beta \in \mathbb{Z}[\sqrt{-3}]$ with $\beta \neq 0$, there exists γ, $\rho \in \mathbb{Z}[\sqrt{-3}]$ such that

$$\alpha = \beta\gamma + \rho \text{ and } \mathrm{N}(\rho) < \mathrm{N}(\beta).$$

Sketch an argument showing that if the only common divisors of α, $\beta \in \mathbb{Z}[\sqrt{-3}]$ are ± 1, then there exist η, $\nu \in \mathbb{Z}[\sqrt{-3}]$ such that

$$\eta\alpha + \nu\beta = 1.$$

iv) Show that if $\alpha|\beta$ for α, $\beta \in \mathbb{Z}[\sqrt{-3}]$, then

$$\mathrm{N}(\alpha) \,|\, \mathrm{N}(\beta)$$

v) Show that 2 does not divide $1 + \sqrt{-3}$ and $1 + \sqrt{-3}$ does not divide 2. Hence conclude that if $\alpha \in \mathbb{Z}[\sqrt{-3}]$ divides both 2 and $1+\sqrt{-3}$, $\alpha = \pm 1$.

vi) Show that there does not exist $\eta, \xi \in \mathbb{Z}[\sqrt{-3}]$ such that

$$2\eta + (1 + \sqrt{-3})\xi = 1$$

Hint: Parity

vii) Conclude that Euclidean division is not possible in $\mathbb{Z}[\sqrt{-3}]$, i.e. given α, $\beta \in \mathbb{Z}[\sqrt{-3}]$ with $\beta \neq 0$, there does not necessarily exist γ, $\rho \in \mathbb{Z}[\sqrt{-3}]$ such that

$$\alpha = \beta\gamma + \rho \text{ and } \mathrm{N}(\rho) < \mathrm{N}(\beta).$$

Solution 11

i) The sum of two elements of $\mathbb{Z}[\sqrt{-3}]$ is clearly in $\mathbb{Z}[\sqrt{-3}]$. To see that the product is an element of $\mathbb{Z}[\sqrt{-3}]$, note that

$$(a + b\sqrt{-3})(c + d\sqrt{-3}) = (ac - 3bd) + (ad + bc)\sqrt{-3} \in \mathbb{Z}[i]$$

for $a, b, c, d \in \mathbb{Z}$.

We say that $\alpha|\beta$ if there exists $\gamma \in \mathbb{Z}[\sqrt{-3}]$ such that $\beta = \alpha\gamma$.

ii) Suppose $\mathrm{N}(a + b\sqrt{-3}) = 1$. Then

$$1 = a^2 + 3b^2 \geq a^2.$$

Hence $a \in \{0, \pm 1\}$. If $a = \pm 1$, then we must have $b = 0$. If $a = 0$, and $b = 0$, then $\mathrm{N}(a + b\sqrt{-3}) = 0 \neq 1$, but if $b \neq 0$, then

$$\mathrm{N}(b\sqrt{-3}) = 3b^2 \geq 3 > 1.$$

Thus, if $\mathrm{N}(\alpha) = 1$, $\alpha = \pm 1$.

iii) It is easy to see that $\mathrm{N}(\alpha) = 0$ if and only if $\alpha = 0$. Similarly to the case of Gaussian integers, if $\alpha = \beta\gamma + \rho$, then

$$\mathrm{Div}(\alpha, \beta) = \mathrm{Div}(\beta, \rho).$$

As $\mathrm{N}(\rho) < \mathrm{N}(\beta)$, we can execute the Euclidean algorithm, which must eventually terminate as the norm of the remainders is a strictly decreasing sequence of non-negative integers. In particular, if the only common divisors of α and β are ± 1, then one of the remainders must be ± 1. Running Euclid's algorithm backwards, we construct $\eta, \xi \in \mathbb{Z}[\sqrt{-3}]$ such that

$$\alpha\eta + \beta\eta = \pm 1.$$

We can ensure this is equal to 1 by sending $(\eta, \xi) \mapsto (-\eta, -\xi)$ if necessary.

iv) If $\alpha|\beta$, there exists $\gamma \in \mathbb{Z}[\sqrt{-3}]$ such that

$$\beta = \alpha\gamma \text{ and hence } \overline{\beta} = \overline{\alpha\gamma}.$$

Thus

$$\mathrm{N}(\beta) = \beta\overline{\beta} = \alpha\gamma\overline{\alpha\gamma} = \mathrm{N}(\alpha)\,\mathrm{N}(\gamma)$$

which implies that $\mathrm{N}(\alpha)|\,\mathrm{N}(\beta)$.

v) As $\mathrm{N}(2) = \mathrm{N}(1+\sqrt{-3}) = 4$, if one of them divides the other, the quotient must have norm 1, and hence is equal to ± 1, which is clearly not true.

If α is a common divisor, then it must have norm dividing $\mathrm{N}(2) = \mathrm{N}(1+\sqrt{-3}) = 4$. By direct inspection,

$$a^2 + 3b^2 = 2$$

has no integer solutions, and so there are no elements of norm 2. Similarly, the only solutions to

$$a^2 + 3b^2 = 4$$

are $(\pm 2, 0)$ and $(\pm 1, \pm 1)$, the only elements of norm 4 are ± 2 and $\pm 1 \pm \sqrt{-3}$, which cannot be common divisors, by essential the same arguments as before.

vi) Suppose there exist $a, b, c, d \in \mathbb{Z}$ such that

$$2(a + b\sqrt{-3}) + (1 + \sqrt{-3})(c + d\sqrt{-3}) = 1.$$

This is equivalent to

$$(2a + c - 3d) + (b + c + d)\sqrt{-3} = 1$$

and hence

$$2a + c - 3d = 1 \text{ and } 2b + c + d = 0$$

Considering these modulo 2, we must have

$$c + d \equiv 1 \pmod{2} \text{ and } c + d \equiv 0 \pmod{2}$$

which is impossible. Hence, so such $a, b, c, d \in \mathbb{Z}$ exist, and therefore no such $\eta, \xi \in \mathbb{Z}[\sqrt{-3}]$ exists.

vii) From parts (iii) and (v), if Euclidean division exists, there exist $\eta, \xi \in \mathbb{Z}[\sqrt{-3}]$ such that

$$2\eta + (1 + \sqrt{-3})\xi = 1$$

Part (vi) says no such η, ξ exist. Thus, Euclidean division is not possible.

Exercise 12 *Steps towards four squares - Quite hard*

Recall that the quaternions

$$\mathbb{H} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\}$$

is equipped with multiplication determined by

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1.$$

Define $\mathbb{H}_{\mathbb{Z}}$ to be the subset of $\mathbb{H}$ consisting of

$$a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$$

such that either $a, b, c, d \in \mathbb{Z}$ or $a - \frac{1}{2}, b - \frac{1}{2}, c - \frac{1}{2}, d - \frac{1}{2} \in \mathbb{Z}$.

i) Show that $\mathbb{H}_{\mathbb{Z}}$ is closed under addition and multiplication

ii) Show that the norm

$$\mathrm{N}(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) := (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k})$$

takes integer values.

iii) Show that $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$ for all $\alpha\beta \in \mathbb{H}_{\mathbb{Z}}$.

iv) Show that, for any $a, b, c, d \in \mathbb{Z}$, there exist $A, B, C, D \in \mathbb{Z}$ such that

$$A^2 + B^2 + C^2 + D^2 = \left(a + \frac{1}{2}\right)^2 + \left(b + \frac{1}{2}\right)^2 + \left(c + \frac{1}{2}\right)^2 + \left(d + \frac{1}{2}\right)^2$$

Hint: For any $a \in \mathbb{Z}$, there exists $a' \in \mathbb{Z}$ such that $a + \frac{1}{2} = 2a' \pm \frac{1}{2}$. This means we can write the right hand side as the norm of

$$2a\prime + 2b'\mathbf{i} + 2c'\mathbf{j} + 2d'\mathbf{k} + \omega$$

for a quaternion ω of norm 1.

Can we write the right hand side in the form $\alpha\overline{\omega}\omega\overline{\alpha}$?

With these results, to prove Lagrange's 4-squares theorem, we just need to prove that every prime is a norm of an element of $\mathbb{H}_{\mathbb{Z}}$.

Solution 12

i) $\mathbb{H}_\mathbb{Z}$ is clearly closed under addition. We have that

$$\begin{aligned}&(a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k})(e+f\mathbf{i}+g\mathbf{j}+h\mathbf{k})\\ =&x+y\mathbf{i}+z\mathbf{j}+w\mathbf{k}\end{aligned}$$

where

$$\begin{aligned}x&=ae-bf-cg-dh,\\ y&=af+be+ch-dg,\\ z&=ag+ce-bh+df,\\ w&=ah+de+bg-cf.\end{aligned}$$

We then have to manually check every possibility. If $a,b,c,d,e,f,g,h\in\mathbb{Z}$, then $x,y,z,w\in\mathbb{Z}$.

In the product

$$(a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k})(e+\frac{1}{2}+(f+\frac{1}{2})\mathbf{i}+(g+\frac{1}{2})\mathbf{j}+(h+\frac{1}{2})\mathbf{k})$$

each of x,y,z,w is an integer plus one of

$$\frac{a\pm b\pm c\pm d}{2}$$

which are either all integers, or all an integer plus $\frac{1}{2}$.

In the product

$$(a+\frac{1}{2}+(b+\frac{1}{2})\mathbf{i}+(c+\frac{1}{2})\mathbf{j}+(d+\frac{1}{2})\mathbf{k})(e+\frac{1}{2}+(f+\frac{1}{2})\mathbf{i}+(g+\frac{1}{2})\mathbf{j}+(h+\frac{1}{2})\mathbf{k})$$

each of x,y,z,w is of the form

$$\begin{aligned}&N+\frac{a\pm b\pm c\pm d\pm e\pm f\pm g\pm h}{2}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4}\\ =&N+1+\frac{a\pm b\pm c\pm d\pm e\pm f\pm g\pm h}{2}\end{aligned}$$

so some integer N, and we again obtain that either $x,y,z,w\in\mathbb{Z}$ or $x,y,z,w\in\mathbb{Z}+\frac{1}{2}$.

ii) Note that

$$\mathrm{N}(\alpha) = a^2 + b^2 + c^2 + d^2 \in \mathbb{Z}$$

for

$$\alpha = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}.$$

if $a, b, c, d \in \mathbb{Z}$. Similarly, for

$$\alpha = a + \frac{1}{2} + (b + \frac{1}{2})\mathbf{i} + (c + \frac{1}{2})\mathbf{j} + (d + \frac{1}{2})\mathbf{k}$$

we get

$$\mathrm{N}(\alpha) = a^2 + b^2 + c^2 + d^2 + a + b + c + d + 1 \in \mathbb{Z}.$$

iii) Oh dear:

$$\begin{aligned} x^2 + y^2 + z^2 + w^2 =& a^2e^2 + b^2f^2 + c^2g^2 + d^2h^2 \\ &+ a^2f^2 + b^2e^2 + c^2h^2 + d^2g^2 \\ &+ a^2g^2 + c^2e^2 + b^2h^2 + d^2f^2 \\ &+ a^2h^2 + d^2e^2 + b^2g^2 + c^2f^2 \\ =& (a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2) \end{aligned}$$

as all the cross terms magically cancel.

iv) The right hand side is

$$\mathrm{N}\left(a + \frac{1}{2} + (b + \frac{1}{2})\mathbf{i} + (c + \frac{1}{2})\mathbf{j} + (d + \frac{1}{2})\mathbf{k}\right).$$

As noted in the hint, we can rewrite this as

$$\mathrm{N}\left(2a + 2b\mathbf{i} + 2c\mathbf{j} + 2d\mathbf{k} + \omega\right)$$

where we have dropped the primes. Let

$$\alpha = 2a + 2b\mathbf{i} + 2c\mathbf{j} + 2d\mathbf{k} + \omega.$$

Then, as $\overline{\omega}\omega = 1$

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

Hence, it would suffice to show that $\alpha\overline{\omega}$ has integer coefficients. But

$$\begin{aligned}\alpha\overline{\omega} &= 2(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})\overline{\omega} + 1\\ &= 2(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})\left(\frac{\pm 1 \pm \mathbf{i} \pm \mathbf{j} \pm \mathbf{k}}{2}\right) + 1\\ &= (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})\left(\pm 1 \pm \mathbf{i} \pm \mathbf{j} \pm \mathbf{k}\right) + 1\end{aligned}$$

which has integer coefficients! Thus we are done!