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

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

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

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 $a|_{\mathbb{Z}[i]}b$.

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

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) $\alpha = 19 + 12i$.

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 $a^{\frac{p-1}{2}} \equiv \pm 1$ (mod p) for every integer a. As such, given $a \in \mathbb{Z}$ such that $a^{\frac{p-1}{2}} \equiv -1$ (mod p), for $p \equiv 1$ (mod 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.

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 $834^2 \equiv -1 \pmod{1993}$

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

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

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.

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.

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 $\alpha,\, \beta \in \mathbb{Z}[\sqrt{-3}]$ with $\beta \neq 0$, there exists $\gamma,\, \rho \in \mathbb{Z}[\sqrt{-3}]$ 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 $\alpha,\, \beta \in \mathbb{Z}[\sqrt{-3}]$ are ±1, then there exist $\eta,\, \nu \in \mathbb{Z}[\sqrt{-3}]$ such that

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

iv) Show that if $\alpha|\beta$ for $\alpha,\, \beta \in \mathbb{Z}[\sqrt{-3}]$, 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 $\alpha,\, \beta \in \mathbb{Z}[\sqrt{-3}]$ with $\beta \neq 0$, there does not necessarily exist $\gamma,\, \rho \in \mathbb{Z}[\sqrt{-3}]$ such that

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

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 $\mathbb{H}_{\mathbb{Z}}$.