MATH7421 Exam Information

The Algebraic Number Theory part of the exam will will feature a handful of multi-part questions (covering the content of Chapters $1-5$ of the notes).

Parts of each question will feature a mix of definitions, proofs and computation (details provided below). Always be as precise as possible and provide full working out. Any valid method of doing computations will be awarded marks, unless the question asks for a specific algorithm to be used.

A calculator is allowed in the exam and a Useful Information sheet will also be provided (which will also be included on moodle in advance of the revision session). Despite this, I will try and make sure that any necessary calculations feature small numbers.

A mock exam will also be provided in advance of the revision session, so that you can see the overall style of the questions and have a go yourself before we meet up. However, note that it is impossible for all topics to be examined in the time available...so do not assume that the real exam will feature exactly the same content as the mock exam!

As always, there might be a couple of parts of questions that are unseen. These are there to test your problem solving skills and your ability to use results from the course in unfamiliar territory. There are many extra exercises that we didn't have time to do in the tutorials...so it's worth going back and getting some practice!

Below is a list of core skills covered in each relevant chapter of the notes. Practicing these skills in advance will give you a much easier time in the exam. (Although as mentioned above, you will need to be able to apply your knowledge too!)

If you have any questions at all, about either the content of the course or the format of the exam, then please get in touch!

1 Introduction: Solving Integer Problems using Commutative Rings

This section looks like there isn't much to know but don't be fooled, it's the most important...since this is full of number theoretic applications/motivations. Practice these skills well!

1. Demonstrate the usefulness of techniques of algebraic number theory in solving number theoretic problems of a Diophantine nature, e.g. Pythagorean Triples, Pythagorean Triples, Pell's Equation, primes of the form $p = x^2 + y^2$).
2. Adapt these methods to unseen number theoretic problems.

2 Polynomials, Roots and Irreducibility

1. Understand basic properties of polynomials, e.g. degree, roots, divisibility, reducibility.
2. Apply reducibility tests to low degree polynomials over $\mathbb{Q}$ and $\mathbb{Z}$, i.e. brute force, use of field extensions, Rational Root Test, Gauss' Lemma, Eisenstein's Criterion

3 Number Fields and their Rings of Integers

1. Define the notions of algebraic number, minimal polynomial, number field, degree.
2. Prove that the minimal polynomial of an algebraic number is irreducible (Theorem 3.10).
3. Prove that if α has degree d then $\mathbb{Q}(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + ... + a_{d-1}\alpha^{d-1} \mid a_i \in \mathbb{Q}\}$ (Theorem 3.11).
4. Compute the minimal polynomials of certain low degree algebraic numbers, describe the corresponding number field and give the degree.
5. Define and compute conjugates of an algebraic number and the real/complex embeddings of a number field.
6. Compute norms and traces of elements in low degree number fields.
7. Prove various properties of norms and traces (Lemma 3.22) (with reminder of the assumptions made within part (d) of the proof).
8. Define the notions of algebraic integer and ring of integers
9. Prove that the ring of integers of a number field has a basis (Theorem 3.36) (The fact used in the proof is provided on the Useful Information Sheet).
10. Compute the ring of integers of low degree number fields (with significant aid in the cubic and higher degree cases).

4 Factorization in Rings of Integers

1. Define the notions of integral domain, irreducible element, prime element, unit, ideal and principal ideal.
2. Prove that Noetherian rings (such as $\mathcal{O}_K$) admit factorisation into irreducibles (Theorem 4.13). (The Noetherian criteria will be given on the Useful Information Sheet).
3. Define what it means for two factorisations into irreducibles to be equivalent, hence what it means to be a Unique Factorisation Domain.
4. Be able to prove that certain low degree rings of integers are not UFD's by giving two inequivalent factorisations of an element into irreducibles, with full justification.
5. Prove that an integral domain is a UFD if and only if every irreducible is prime (Proposition 4.25).
6. Define what it means to be a Euclidean Domain and understand that every Euclidean Domain is a UFD.
7. Prove that certain low degree number fields have rings of integers that are Euclidean Domains under their norm maps, hence that they are UFD's.

5 Dirichlet's Unit Theorem

1. Prove that units in rings of integers are those elements satisfying $N(\alpha) = \pm 1$ (Lemma 5.3).
2. Prove that if $d > 1$ is non-square and there exists a unit $v \in \mathbb{Z}[\sqrt{d}]\backslash\{\pm 1\}$ then $\mathbb{Z}[\sqrt{d}]^\times = \{\pm v^m \,|\, m \in \mathbb{Z}\}$ (more general result than Theorem 5.7 but identical proof).
3. Compute unit groups of rings such as $\mathbb{Z}[\sqrt{d}]$ and $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, by finding an explicit fundamental unit, with full justification.
4. State Dirichlet's Unit Theorem in generality and use it to predict the structure of unit groups of rings of integers in number fields (without being expected to give explicit fundamental units).
5. Understand how Dirichlet's Unit Theorem for the ring $\mathbb{Z}[\sqrt{d}]$ is related to solutions to Pell's equation $x^2 - dy^2 = \pm 1$. Use this relationship to describe the set of solutions and to generate explicit solutions.

The content of the Fermat's Last Theorem section is non-examinable.