MA40238 NUMBER THEORY 2014/15 SEMESTER 1 EXAM INFORMATION

ZIYU ZHANG

1. General Information

As you have experienced in many other exams, there will be four problems in the exam, each worth 20 marks. Your best-answered three problems contribute towards the assessment. University-supplied calculators will be allowed. The following chart shows the material covered in each problem.

Problem number	Material covered
problem 1	weeks 1-3
problem 2	weeks 4-5
problem 3	weeks 6-8
problem 4	weeks 9-10

2. Types of Questions

Each problem is a combination of questions of the following five types.

2.1. **Definitions.** Definitions are always the building blocks in any branch of mathematics. Make sure you know the precise definitions of the mathematical concepts we learned in this unit. Roughly 20% of the marks are given to this type of questions. Here are some sample questions:

- What does it mean to say a divides b, where a and b are integers, $a \neq 0$?
- Define the Dirichlet product of two arithmetic functions f and g.

2.2. **Statements of Results.** Mathematical results, such as lemmas, propositions, theorems, corollaries and formulas are the main outcome of any mathematical research. It is necessary that you can precisely state all results we learned in lectures, understand their relations, and use them to deduce some simple consequences. You could be asked to state a result by its name, or by its function, or by an explicit example. Roughly 20% of the marks are given to this type of questions. Here are some sample questions:

Date: November 30, 2014.

- State the Möbius inversion theorem.
- State a lemma proved in class, concerning a criterion for algebraic integers, which can be used to prove that the sum and product of two algebraic integers are still algebraic integers.
- Determine whether $\sqrt{2}+\sqrt{3}$ is an algebraic integer. Explain your reasoning. If you use any result proved in class, state it clearly.
- Write down the set of all algebraic integers in the field of rational numbers $\mathbb{Q}$.

2.3. **Standard Calculations.** Doing explicit calculations is a basic skill that one should learn from any mathematical course. We have seen many examples of such calculations either in lectures or in exercise sheets. Make sure you know how to do them, and be very careful when you manipulate numbers. You need to show all you calculation to get full marks. Roughly 20% of the marks are given to this type of questions. See Appendix A for a list of such calculations that you need to know. Here are some sample questions:

- Solve the congruence equation $6x \equiv 44 \pmod{26}$.
- Compute the Legendre symbol $(\frac{474}{733})$.
- Compute the discriminant of the quadratic field $\mathbb{Q}(\sqrt{5})$.
- Compute the class number of the quadratic field $\mathbb{Q}(\sqrt{5})$.

2.4. **Proofs of Important Results.** Understanding the proofs of important results is usually very helpful for understanding the results themselves, and is usually a starting point for carrying out mathematical research. You will be asked to write down some of the proofs that we learned in lectures. Roughly 20% of the marks are given to this type of questions. Some of the proofs are very short, while others are longer, in which case you could be asked to prove a certain step in it. See Appendix B for a list of proofs that you need to understand. The best strategy for learning a proof is to think it through and make sure you understand a few key steps, then try to write the whole proof down in your own words. Here are some sample questions:

- State and prove Gauss' Lemma for Legendre symbols.
- Prove that there are infinitely many positive primes in $\mathbb{Z}$.

2.5. **Mysterious Questions.** The last question in each of the four problems is worth 4 marks, which is 20% of the total marks. You may or may not have seen them in lectures or exercises, but the techniques required to solve these problems should all be familiar. If you cannot solve such a problem at the first glance, try to think which results or examples you have learned in lectures or exercises are likely to be related to the question at hand, and how you can apply them in the question. Even if you cannot solve such a problem completely, you should still write down the steps that you have done to earn partial marks. In the end, these questions are not difficult, so please do not be afraid!

Appendix A. List of Standard Calculations

You need to know how to do the following types of standard calculations.

- Find the highest common factor of two integers by Euclidean algorithm.
  Sample question: Use Euclidean algorithm to compute $\mathrm{hcf}(963, 657)$ and find a pair of integers m, n satisfying $963m + 657n = \mathrm{hcf}(963, 657)$.
- Calculate the explicit values of the follow arithmetic functions: ν, σ, μ and ϕ.
  Sample question: Compute $\phi(360)$.
- Solve a linear congruence equation.
  Sample question: Solve the congruence equation $9x \equiv 6 \pmod{15}$.
- Solve a linear Diophantine equation with two variables.
  Sample question: Find all integer solutions to the equation $9x + 15y = 6$.
- Solve system of linear congruence equations.
  Sample question: Solve the system of equations $\begin{cases} x \equiv 31 \pmod{41}, \\ x \equiv 59 \pmod{26}. \end{cases}$
- Find primitive roots and number of generators in a cyclic group.
  Sample question: Show that 2 is a primitive root modulo 29. How many generators does $\mathbb{Z}_{29}^*$ have?
- Compute a Legendre symbol.
  Sample question: Compute the Legendre symbol $(\frac{1003}{1151})$.
- Find all primes for which a certain number is a quadratic residue.
  Sample question: Find all odd primes for which 3 is a quadratic residue.
- Use Gauss' Lemma to compute a Legendre symbol.
  Sample question: Use Gauss' Lemma to compute the Legendre symbol $(\frac{4}{7})$.
- Determine whether a given complex number is an algebraic integer (using definition or any criterion proved in class).
  Sample question: Determine whether $3 + i$ is an algebraic integer.
- Compute the trace and norm of a certain element in a number field.
  Sample question: Compute the trace and norm of $\frac{1}{2}(1 + \sqrt{5})$ in $\mathbb{Q}(\sqrt{5})$.
- Compute the discriminant of some elements in a number field and the discriminant of a quadratic field.
  Sample question: Let $K = \mathbb{Q}(\sqrt{5})$. Compute the discriminant $\Delta(\sqrt{5}, 1 + \sqrt{5})$ and the discriminant Δ_K.
- Compute the norm of a principal ideal in the ring of integers in a number field.
  Sample question: Let $K = \mathbb{Q}(\sqrt{5})$. Let $I = (1 + \sqrt{5})$ be a principal ideal in $\mathcal{O}_K$. Compute $N(I)$.
- Compute the Minkowski bound and class number for a quadratic field.
  Sample question: Compute the class number of the quadratic field $\mathbb{Q}(\sqrt{5})$.

Appendix B. List of Proofs of Important Results

Please be prepared to give the proof of some of the following results. The numbers of these results refer to the lecture notes posted on the unit webpage.

- Proposition 1.21: the formula for $\sum_{d|n} \mu(d)$.
- Theorem 1.26: Möbius Inversion Theorem.
- Proposition 1.28: the formula for $\sum_{d|n} \phi(d)$.
- Proposition 2.5: solvability and number of solutions of a linear congruence.
- Theorem 2.12: Chinese Remainder Theorem.
- Theorem 3.4: any finite subgroup of the group of units in a field is cyclic.
- Corollary 3.5 (assuming Theorem 3.4): $\mathbb{Z}_p^*$ is cyclic for any prime p.
- Proposition 4.4 (1): Euler's criterion for Legendre symbols.
- Proposition 4.5 (assuming Proposition 4.4 (1)): the formula for $(\frac{-1}{p})$ and $(\frac{2}{p})$.
- Lemma 5.1: Gauss' Lemma.
- Proposition 5.4: infinitely many primes congruent to -1 or 1 modulo 4.
- Lemma 6.5: a criterion for algebraic integers.
- Proposition 7.14: discriminants of quadratic fields.
- Proposition 8.8: ascending chain condition.
- Theorem 8.16: unique factorisation of ideals.
- Proposition 9.5: class number is 1 iff $\mathcal{O}_K$ is a PID.
- Theorem 9.11: Minkowski's Theorem.
- Theorem 10.7: class number is finite for quadratic fields.

Appendix C. List of Non-Examinable Exercises

The following exercises are non-examinable.

- Sheet 1: Ex 1.4.
- Sheet 2: Ex 2.3, Ex 2.4.
- Sheet 3: Ex 3.2, Ex 3.3, Ex 3.4.
- Sheet 4: Ex 4.3, Ex 4.4.
- Sheet 5: Ex 5.3, Ex 5.4.
- Sheet 6: Ex 6.3, Ex 6.4.
- Sheet 7: Ex 7.2, Ex 7.4.
- Sheet 8: Ex 8.2, Ex 8.4.
- Sheet 9: Ex 9.4.
- Sheet 10: Ex 10.3, Ex 10.4.