MA40238 NUMBER THEORY (2014/15 SEMESTER 1) EXAM FEEDBACK

ZIYU ZHANG

General Comments

In general, this exam is not very difficult, but comprehensive. It covers all the 21 lectures in the entire semester. Each problem consists of 7 questions. Among them, the first 6 questions are fairly standard. They are mostly asking for definitions, statements and proofs of theorems, and computations. The answers to these questions (or similar questions) can all be found in lectures. The last question in each problem might require deeper understanding of the lecture material and some more creativity.

Many candidates did very well in the exam, which makes the average slightly above 70%. Given the relatively large size of the class, the range of marks is also quite wide, including some very strong scripts and some very weak ones.

Among all the four problems, Problem 2 is the most popular and the best answered problem. This is a bit surprising to me, as I thought this problem contains the longest proof (the proof of Euler's criterion) and the most difficult question (that 7 is a quadratic non-residue modulo $p = 4^n + 1$) in this exam. Problem 4 is not very popular, probably because the material covered in this problem was taught in the last 2 weeks of lectures. However, this problem was also answered very well.

The following are some common mistakes in this exam.

Question 1

The definitions in (a) and (b) were answered well, except that some people could not tell the difference between '$a - b \mid m$' and '$m \mid a - b$'.

I believe that the content of the Chinese remainder theorem should be familiar to everyone. However, to state it correctly, you need to mention that the m_i's are pairwise coprime (or something equivalent). Without this condition the theorem would not hold. Moreover, the uniqueness of solutions is also part of the conclusion, which should not be omitted.

Parts (d) and (e) were answered very well. We did both of them in lectures.

Date: January 27, 2015.

Many people lost marks in part (f). Indeed, the theorem you were asked to state is a difficult one, which itself is a key step in proving $\mathbb{Z}_p^*$ is cyclic. Some people didn't seem to remember which theorem is relevant here, while some other people failed to state it precisely; e.g. forgot to mention the subgroup of K^* is assumed to be *finite*. To use the theorem to prove $\mathbb{Z}_p^*$ is cyclic, you need to mention that $\mathbb{Z}_p$ is a field. Otherwise the theorem cannot apply.

Part (g) is probably new to most people. The proof is actually quite short, but you need to find the right way to argue it. The theorem we need to use here is Fermat's little theorem. It is clear that $n^{q-1} \equiv 1 \pmod{q}$. We also need to show $n^{q-1} \equiv 1 \pmod{p}$. By assumption we can write $q - 1 = k(p - 1)$ for some integer k. Then you immediately have $n^{q-1} = (n^{p-1})^k \equiv 1^k = 1 \pmod{p}$. Many people made a mistake here by saying $n^{q-1} = n^{p-1}n^k$, which is wrong. Obviously these people were confused by the formulas for n^{ab} and n^{a+b}.

Question 2

In part (a), a common mistake is to miss the value 0 when $p \mid a$. Some people lost marks in part (b) because of a similar reason: it is important to mention p and q are distinct primes; otherwise the value of the product $(\frac{p}{q})(\frac{q}{p})$ would be 0 instead of ±1.

The two parts on the computation of Legendre symbols were answered in general well. As mentioned several times in lectures, it is much less likely to mess up the signs by making use of Jacobi symbols to compute Legendre symbols. Some people still used the classical method and made sign mistakes.

Part (e) is a theorem proved in lectures. The proof is not long but involves quite a few ingredients. It shouldn't be confused with the other parallel result (primes congruent to -1 modulo 4), whose statement is similar to this one but proof is very different.

Euler's criterion is a very important result. Its proof consists of three cases. The case of $(\frac{a}{p}) = -1$ is longer than the other two, which some people could not finish.

Part (g) is probably the most difficult question in this exam. To show $(\frac{3}{p}) = -1$, you just need to realise that $p \equiv 1 \pmod{4}$ for using the quadratic reciprocity, and $p \equiv 2 \pmod{3}$ for reducing $(\frac{p}{3})$ to $(\frac{2}{3})$. To show $(\frac{7}{p}) = -1$, besides $p \equiv 1 \pmod{4}$, you also need to realise that $p = 4^n + 1 \equiv 5$ or 3 or 2 $\pmod{7}$. But $p \equiv 2 \pmod{7}$ cannot happen, because this only happens when n is a multiple of 3, which violates the assumption that p is a prime (can you see why?). It remains to show that $(\frac{5}{7}) = (\frac{3}{7}) = -1$. Many people didn't find the right reason to eliminate the case of $p \equiv 2 \pmod{7}$, which is reasonable because this question is new and somewhat tricky.

Question 3

Parts (a) and (b) were answered quite well. It is great that most people can state the definition precisely, including the linear transformation L_α.

The integral basis is probably a difficult concept in this unit. In part (c), an integral basis of $\mathcal{O}_K$ for $K = \mathbb{Q}(\sqrt{d})$ depends on the congruence class of d modulo 4. It should not be confused with a basis of K over $\mathbb{Q}$. Some people simply wrote $\{1, \sqrt{d}\}$ which is not a complete answer. Part (d) relies on the answers in parts (b) and (c), which also depends on the congruence class of d modulo 4.

The three descriptions of the norm of an ideal were mentioned a couple of times in lectures. Different descriptions are useful in different situations hence worth remembering. This question was not answered well as few people remember all three descriptions correctly, especially the second one, which involves integral bases for both $\mathcal{O}_K$ and I.

The ascending chain condition is a very important property of the ring of integers in a number field. This question was in general answered quite well.

Part (g) is a very interesting question. Many people can find the equation for $1+\sqrt{1+\sqrt{5}}$ correctly using the method discussed in lecture, and conclude that it is an algebraic integer. Using the same method, it is also possible to find an equation for $\frac{1+\sqrt{3}}{2}$. However, it is either not a monic polynomial, or has non-integral coefficients. Many people claimed from here that $\frac{1+\sqrt{3}}{2}$ is not an algebraic integer, which is not correct, because this particular polynomial fails to satisfy the requirement of the definition does not explain why no other polynomial works.

In fact, to see $\frac{1+\sqrt{3}}{2}$ is not an algebraic integer, we just need to recall that the only algebraic integers in $\mathbb{Q}(\sqrt{3})$ are $a+b\sqrt{3}$ for any $a, b \in \mathbb{Z}$. Some of you gave other nice proofs without using this fact (e.g. use the norm, or use the ring structure), which are all very good.

Question 4

Parts (a) and (b) consist of two definitions and a standard theorem. Most people answered them correctly. However, there are some details that one has to pay attention to. For instance, in Minkowski's theorem, the conditions *convex* and *centrally symmetric* cannot be omitted, and the conclusion is the existence of a *non-zero* point in the lattice (otherwise the statement is trivial).

Most people remember the formula for Minkowski bound, and use it to prove the finiteness of class numbers correctly.

Parts (e) and (f) are familiar questions, and are well answered. To explain why the ring of integers here is a UFD, one needs to mention two results proved in lectures: having class number 1 is equivalent to being a PID, and every PID is a UFD. This is where some people lose marks.

Part (g) is slightly harder than the last question, but we have seen some similar questions in lectures and exercise sheets. The class number is still 1 because the only ideal of norm 2 is principal. Many people knew that this requires solving a certain equation for integer solutions. But many sign mistakes happened in the computation, especially the sign of the term $7b^2$.