NUMBER THEORY (MA40238): EXAM COMMENTS

These are some comments on the exam at the end of MA40238. They are supposed to be useful feedback for those who sat the exam and guidance for those who are taking the course in the future.

In general this went well. The scatter plot, which plots students scores on this exam against their average score on all their exams, was satisfyingly diagonal, meaning that few of you did better or worse on this unit than you did overall. There were few very weak scripts and some extremely strong ones.

Q1. Usually Question 1 is the most popular, but not this time, despite the revision question on this topic issued shortly beforehand. I got the impression that most people had concentrated on continued fractions at the expense of the early part of the course. Perhaps the forbidding notation put you off, or perhaps you noticed that although most of this question is quite friendly it has a considerable sting in the tail: the rider in part (g). Those who did attempt the question (about 60% of you) mostly got as far as part (e) without problems, though some tripped over (d); but many people couldn't prove the Möbius inversion theorem. Most could state it. Part (f), which is extremely easy, caused many casualties, I'm not sure why – I did it in the lectures but even if I hadn't it would still be easy. However, part (g) is not easy. In fact there were no complete solutions to this question at all: the few who did give complete (let alone correct) solutions to (g) had all skipped (e) or (f), and the best attempts at (g) all stopped short of the end. Nevertheless, I don't think the question was too hard: it was just that people who could do it could also do the other questions, and chose to do them instead.

Q2. Popular question, mostly well done. You do need to notice which parts are asking you about Jacobi symbols (the bottom has to be an odd prime) and which are asking about Legendre symbols. There were some fairly meaningless statements that purported to be Gauss's Lemma, in some cases followed by a correct proof of the correct form of Gauss's Lemma, but the thing that really trapped a lot of people was the clause about not factorising anything in (g). Some people just spotted that $441 = 21^2$: true, but not an answer to the question, and therefore not worth any marks. More people did some standard moves and then got to 121, which is more recognisable as a square because it is in the multiplication tables you are taught at primary school. This got a part score for getting as far as 121. Saying that 4 is a square is all right, though, because you can do that by taking out a factor of 2, which is allowed. The point of all this is that we are

trying to pretend that these are big numbers. If you were asked to compute a Legendre symbol involving 100-bit numbers you wouldn't be able to factorise and you wouldn't bother checking whether the number you have been given is a square, even though that's easy, because a 100-bit number is a square with probability about 2^{-50}.

Q3. The bookwork here is tricky enough to have caused some upsets, especially the little bit of abstract algebra I used to compute the volume in part (c). Just about everybody got somewhere with this question, though. A common mistake towards the end was either to forget the value of Δ (and not be able to work it out again) or to fail to notice that -7 is 1 mod 4, not 3 mod 4. That led to immediate disaster in the last part. Otherwise people who could do the first sentence of part (e) could do all of it. This question worked well: there were a lot of good answers and progress was nearly proportional to understanding.

Q4. This question was generally well done. The main confusion seemed to be between "periodic" and "purely periodic", which surprised me; but it wasn't very widespread. The question is fairly easy but is also quite long, so some people simply didn't reach the end before time ran out; again this is fair enough, as those who understood better were able to work more efficiently and therefore make more progress.

GKS, 12/2/13