PROGRAMMING AND DISCRETE MATHEMATICS (XX10190): EXAM COMMENTS

These are some comments on the May exam at the end of XX10190. They relate only to the questions set by me (GKS), and are supposed to be useful feedback for those who sat the exam and guidance for those who are taking the course in the future.

Look, we don't care what your calculator number is. In the past, the University was terrified that students were going to steal the calculators – of course, nobody ever did – so they printed this terrible warning, copied from a fag packet, about what would happen if you didn't give the number. Then they ordered five years' supply of pink cover sheets. Unfortunately, soon after that, most other departments switched to using answer booklets, so we are having to use up the supply of pink sheets on our own. It will take most of the rest of the century, unless we start admitting even vaster numbers of students than we already do.

So what you should do is ignore the bit about the calculator and instead concentrate on the bits that do matter: not tying up Section A and Section B questions together (start each question on a fresh sheet) and ticking the boxes on the front that say which questions you attempted. This will make the examiner feel much less exasperated, which is what you want.

Overall this exam was not well done. One reason is that it was different in style from the exams of previous years, because the students sitting them had a different version of the textbook, one that didn't contain the exact definitions and bookwork from the lectures. The exam I set was therefore more problem-based, and you didn't have enough similar exams to practise on. Another reason, possibly more important, was that a lot of you didn't come to the lectures, and even fewer to the examples classes.

Q3. This shows you how to calculate Legendre symbols fast. You calculate Jacobi symbols instead: they usually tell you nothing, but if the thing on the bottom is an odd prime, they happen to be the same as the Legendre symbol, which is what you want.

Most of you were able to say what a Legendre symbol is, and so you should be, as it's in the book. Most of you recognised the rule alluded to in part (b) as quadratic reciprocity, but many of you did not do what the question says and write it down. Instead, you wrote down its name, "quadratic reciprocity". However, few people actually lost marks here because they did write it down before using it in part (c). I don't mind if you do the question in a different order.

In part (c), though, the XX10190 pseudoprime made its appearance. This is a number that isn't prime but is treated by candidates as if it were. There were a lot of them, including

28, 0, 555 and, most oddly, 611, which you have just been told is composite. Legendre symbols have odd primes on the bottom: if you wrote anything else, you lost marks. But most people got this one right.

Not so part (d), which, however, is not remotely difficult. Again, it helps to read the question. It suggests using induction on n, not b. There are other ways to do the question, and some of you found them, but induction on n is quick and easy.

The approach to part (e), among people who couldn't do it, was not so much not to read the question as not to pay attention to it. Some of you simply said that $\left[\frac{611}{1109}\right] = \left(\frac{611}{1109}\right)$ and that you had calculated that in part (c). So you had, but you had used the factorisation of 611, which is now forbidden. Others took a copuple of steps before factorising ($121 = 11^2$ came up quite often). Even extracting a factor of 3 is against the rules, and cost marks. The point is that dividing by 2 costs a computer no arithmetic at all (you just slide the number to the right, like dividing by 10 if you are human). Factorisation, even of medium-sized numbers, on the other hand, is expensive.

Q4. Every year some people, asked to explain one of RSA and Diffie-Hellman, explain the other one instead. As the answers are in the book, I have very little sympathy with them. There weren't that many this year. A significant minority, though, could not explain Diffie-Hellman at all. I cannot be certain, but they probably didn't go to the lectures. Most people who could do (a) could also do (b), but there were a few whose created something that was shared but not secret (transmitting it at some stage) or secret but not shared.

The computations in part (c) divided you sharply. Some breezed through them: some stumbled. Those who stumbled often did so because they think that you compute 36^{13} mod 83 by computing 36^{13}, dividing it by 83 and noting the remainder. That's a bit like finding out how many penny coins you have in your pocket by going to a bank, changing all your banknotes into pennies, counting the number of pennies you now have and noting the remainder when you divide by 500. I explained this in the lectures and I showed you an example of how to do the calculation in one of the examples classes. But you didn't go to the examples classes, did you, because that's not really part of the course. So of course you missed the example that came up in the exam, so you didn't do as well as the people who did go to the examples class. If you think that is unfair you need to reset your brain.

Parts (d) and (e) confused people, but they aren't difficult. Telling Fred anything is always a bad idea, of course; but you can't avoid telling Fred things except by never telling anybody anything, because you can't recognise Fred. So you have to think about what the consequences are. One way to do this is to think what would happen if Bob were Fred, as he might be. If what Fred knows is only what Bob knows, then Bob could do as much

damage as Fred could; and if he is Fred, he'll do it. So telling Fred that much can't make the situation any worse.

5. This should have been easy and I don't really know why it wasn't. The first part is bookwork (and you've got the book...) and the second very nearly so. Part (c) checks that you understood what you wrote in (b) by asking you to do an example. Most of you did not understand what you had written in (b), even when it was right, which it often wasn't. You usually got part of the way. Part (d) really did require understanding, which is the point: you shouldn't be able to score very high without a good idea of what is going on. However, a lot of people wrote down things that were not diagonal and claimed they were Δ_4 or, even more often, things that had far too many non-zero entry and claimed they were P.

GKS, 21/7/15