PROGRAMMING AND DISCRETE MATHEMATICS (XX10190): EXAM COMMENTS

These are some comments on the 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.

Generally people have now worked out how to handle the exam paper. Only two of you accidentally revealed your names by getting the pink paper wrong, only two handed Section B questions to the Section A examiner, and none tied a knot in the treasury tag. You almost all dutifully wrote in your calculator number, which we don't care about, and half of you didn't tick the boxes saying which questions you have answered, which we do care about.

Q3. Not one of your better efforts. If you are asked to say what a code is you have to say what a code is. I'm not just asking you for the dimensions: I want to know what they are the dimensions of. It's no use saying "C has dimension n and V has dimension n" if you don't say what kind of thing C is or what V is at all. Some of you talked about the dimension of $\mathbb{F}_2$, which makes no sense at all. I didn't care, though, if you got m and n the wrong way round. Some sources talk about a $(7,4)$ code and some about a $(4,7)$ code and I am not sure that I was consistent, so I can't complain if you weren't. But it doesn't matter, because m and n are just two numbers, one bigger than the other, and it makes no difference what order we list them in. Then some of you insisted on inserting minima into part (b), and some of you made no mention of C in part (c). That means you weren't reading the question. Part (d) split you into those who knew what you were talking about and those who didn't, about half of each; but when it says "Show" in a question you have to write some mathematics. The last two parts, though, were better done and as a result most people scored not too badly on this question.

Q4. Most of you can explain RSA fairly clearly, though there were some spectacular failures. As usual, a small proportion blithely wrote about Diffie-Hellman instead and scored zero as a result. Some gave no detail or insufficient detail but on the whole the first part of this question was well done.

The second part was not. Some of you recognised ABBA, whose relevance for us is purely that they have names beginning with A and B. A few quoted the lyrics in your answers. Maybe more than a few: not being much of an ABBA fan myself, I might not have noticed, but I suspect that ABBA lyrics are quite easy to distinguish from cryptography. Most people dealt with (a) without problems, and the first part of (b) (apart from some linguistic confusion caused by double negatives), but not everybody had the correct reaction to the sight of two non-coprime integers, which is to use Euclid's algorithm to take their hcf. Some of you tried to use the Chinese remainder theorem, which is careless because the next part of the question effectively reminds you that the Chinese remainder theorem is for when you do have coprime integers. To do (c) correctly, you need the Chinese remainder theorem in its entirety: it doesn't just say that simultaneous congruences have solutions, it tells you how to find the solutions and it tells you what the other solutions are once you've got one. Almost nobody said this cleanly, although some of you pieced it together. And that made the very simple trick in the last part hard to spot; but this was meant to be hard, so that's all right.

What nobody spotted is that the question is wrong, sort of. The thing is that a is supposed to be coprime to $\varphi(N_1)$, but $\varphi(N_1)$ is even so we can't take $a = 2$. In fact, this doesn't matter. It only causes trouble when you try to decrypt, and the question doesn't require you to do that so the difficulty never shows up. Also, in reality, you can use $a = 2$, because what happens is that when Agnetha tries to take square roots mod N_1 at the end she gets two possible answers (at least, if she has taken $p_1 \equiv q_1 \equiv 3 \bmod 4$). Well, four, actually, but we can ignore ± 1. So she gets two possible messages from Benny: one is an ABBA lyric, and the other is gibberish, so she shouldn't have any difficulty telling which is which. Should she?

5. You did very badly at the start. If it says "define" you have to define: your answer must begin "K^* is..." or $K^* = \{\ldots$". And if you are asked to prove that something is a subgroup of something else, you have to prove it is a subgroup, not a subset. And no, you can't ignore inverses. $\mathbb{N}$ is not a subgroup of $\mathbb{Z}$. And no, it doesn't say that K is finite. It could perfectly well be $\mathbb{C}$. So any answer that begins "Let the order of K be n" is wrong. So is an answer that refers to "the field K^*": it isn't a field, although K is. The words "field" and "group" have precise meanings and you mustn't use them unless the object you are calling a field or group actually is one.

As for (b), far too many of you don't know what the order of a group is. Lots of you assumed that n is prime, sometimes just out of habit and sometimes because you genuinely thought it has to be. Those who did know that it doesn't have to be prime often thought that $\mathbb{F}_n$ is the same thing as $\mathbb{Z}/n$. It isn't. If p is prime then $\mathbb{F}_p \cong \mathbb{Z}/p$ but if n is composite (it has to be a prime power, which doesn't help you in this question) then $\mathbb{F}_n$ is NOT the same as $\mathbb{Z}/n$. You can tell, because $\mathbb{Z}/n$ isn't a field, so you mustn't call it a field. But just because you know one thing with n elements that isn't a field, that doesn't mean there isn't something else with n elements that is.

After that it got better. Your explanations of Diffie-Hellman were mostly fairly sound, though often lacking an important detail. Again, a few people wrote about RSA instead and scored zero. You might expect that they would be the same as the people who had written about Diffie-Hellman in Q4 but no, those people simply wrote about Diffie-Hellman again, scoring some marks this time. Beyond that it was actual calculation, and people either got it right or followed their own wrong version of Diffie-Hellman. Mostly that meant forgetting that messages are mod p but because $(\mathbb{F}_p^*)^2$ has order q, the keys are mod q.
However, there is one important thing that a lot of you got wrong. The keys are integers mod q, not elements of $(\mathbb{F}_p^*)^2$. It does not make sense to raise an element of a group to the power of anything but an integer. You can't write g^h where g and h are in the same group (well, you can, but it means something else): you can only write g^a where $a \in \mathbb{Z}$, and that means $g.g \dots g$ (a times). However, if the order of the group is q, then $g^q = 1$ always, so what g^a is depends only on what a is mod q: that is, $g^a = g^{a+\lambda q}$ for any $\lambda \in \mathbb{Z}$. So in that case it does make sense to talk about raising g to the power a where $a \in \mathbb{Z}/q$, but only for q, the order of the group. So your keys should be in $\mathbb{Z}$, but since a and $a + \lambda q$ have the same effect, I may as well not tell you λ and just say what my key is mod q; so the keys are in $\mathbb{Z}/q$. But $\mathbb{Z}_q$ is not the same thing as $(\mathbb{F}_p^*)^2$, even though they are both cyclic groups of order q: if I think of $\mathbb{F}_p$ as $\mathbb{Z}/p$ then an element of $(\mathbb{F}_p^*)^2$ is an integer mod p, not mod q.

GKS, 10/6/14