XX10190: Feedback on Section B of the May exam

Q3. That was awful. Really dire. If you had all got the same things wrong then it would probably be my fault, but it wasn't like that.

The first thing is that m^a means "mutiply m by itself a times". So a has to be an integer, because you are counting something. It's not an element of the group G that m belongs to. Lots of you tried to raise an element $m \in \mathbb{F}_p$ to the power of $a \in \mathbb{F}_p$, which makes no sense. If what you are writing does not mean anything, it is going to score zero.

A slight complication is that if you know that the order of G is k then it only matters what a is mod k, so you can think of a as being in $\mathbb{Z}/k$, but that's only if k is the order of G. In this case G is $\mathbb{F}_p^*$ (remember that $\mathbb{F}_p$ is $\mathbb{Z}/p$) so $k = p - 1$, which is not p. So any answer that started by telling Alice to choose $a \in \mathbb{F}_p$ is wrong. So is an answer that tells her to choose $a \in \mathbb{F}_p^*$, because $\mathbb{F}_p^*$ is all the non-zero elements of $\mathbb{Z}/p$. Non-zero elements of $\mathbb{Z}/p$ are not elements of $\mathbb{Z}/(p-1)$. There are $p - 1$ of each, but that doesn't make them the same things.

You can't invent notation. Well, you can, but then you must say what it means. Don't write $\mathbb{F}_* p$ or $\mathbb{F}_*^p$ as if they were the same thing as $\mathbb{F}_p^*$.

Some people were confused about what is sending a message and what it creating a shared secret. If Alice chooses something and conveys it to Bob, that's a message. If she doesn't choose it, it's a shared secret.

The actual calculation mostly reasonable well done by those who knew what they were doing, and even by some who didn't: one of you wrote "This is clearly wrong [sad face emoji]" at the bottom of a completely correct solution (which still gets full marks). You need to be able to handle indices correctly, though. And not write numbers in the millions. A bit of karma here: if you ask a university calculator to work out 8^{65} mod 83 it overflows and you get 0. That is blatantly the wrong answer, but several people carried on regardless. Not believing your calculator is a basic life skill for a mathematician.

The discrete log problem is the problem of taking discrete logs. It may or may not be difficult: that depends on what you are taking discrete logs in.

A lot of you simply didn't know what a discrete log is. At this point I started to lose sympathy. You were told in the lectures, it was on the examples sheets and it's been asked on the exam three times in the last five years. If you looked at any of those things you would know.

Again, you have to make sure that what you write is meaningful. For example, one of you wrote this (if it was you, I apologise: I simply picked an example, and there were many other people who wrote similar things):

The Dlog problem is for a key a and a generator g $\exists h = g^a$ [squiggle] $(a = \log_g h)$ Where Eve wants to find key a.

This scored one out of two, which was very generous. One problem with it is that you haven't bothered to say what h is. A more serious problem is that it is completely ungrammatical. I don't know what you think $\exists$ means, but it actually means "there exists". You are not allowed to use it to mean anything else, such as "does there exist?" (which wouldn't make sense either here). Mathematical writing is about being precise with language, and this sort of thing is anything but precise.

In part (d) there was some credit for mentioning the Chinese Remainder Theorem, but to get much more that you needed to say what it gives you. Some people did, but then many jumped from something mod rs to something mod $p - 1$ (or, worse, mod p).

Few of you saw Alice's extremely sneaky dodge in the last part, but few were still standing by that stage anyway.

Q4. Better. Most of you know what a code is, but too many of you write nonsense. Example: *$(m-n)$-code is the subgroup of $\mathbb{F}$ in the dimension n over the field $\mathbb{F}_2^m$*. (Again, please do not take personal offence if that was you. I can't write this kind of thing myself, so I have to borrow from somebody who can.) This sentence tells me that you do not know what a group is, or a field or a vector space, you do not know what $\mathbb{F}_2$ is and you do not understand the term "dimension". So you score zero, but also you have already persuaded me that anything you write that looks close to being meaningful, probably isn't actually meaningful.

Most of you wrote less concentrated nonsense than that. You tended to write things like *a subspace over* rather than *a subspace of*, which may not seem too serious but reveals confusion about what a field is

and what a vector space is. Some of you failed to mention m or n in your answer to (a) or failed to mention C in your answer to the last part of (b): obviously, that's not good.

Less seriously, some of you got m and n the wrong way round. I let this pass, because the question doesn't remind you that the convention is $m > n$ and there is no particular reason why it is that way round rather than the other.

The majority of you can define the Hamming distance, weight and minimum distance, but some of you told me things like x_i *with* $i \in \mathbb{F}_2$ or failed to distinguish between a set and the size of the set. This tripped you up in part (c), although not always enough to matter: in general, (c) was done well. Not so (d), which a lot of you simply skipped. Those who tried and got it wrong mostly fell over the notation, but what a lot of you did was to ramble vaguely without actually writing down anything definite enough to be wrong. This scored zero.

About half of you who tried could compute the check matrix (a few computed the decoder matrix instead, which is no good) but part (f) revealed that a significant proportion of those do not know what the check matrix is for. Some got everything right but gave a final answer were the corrected message is the same as the original one but for one pair of entries swapped. Sorry, but that's two changes, not one.

A more serious problem, less widespread though, was to start talking about parity bits. This happened because you weren't paying attention and remembered only one example, as if all codes were the parity bit code. And that's quite serious, because it is the same mistake as thinking that you can prove a statement by giving an example of when it is true, which is a basic logical error that you should not be making.

Q5. There weren't all that many serious attempts at this one, which was a pity given the standard of attempts at Q3. Most attempts were either successful or simply stopped suddenly: you didn't write much that was actually wrong. Some of you wrote something called ζ and didn't say what it is, which didn't do you much good. A lot of people sinply skipped the off-diagonal case in part (a), which is of course where most of the marks were. Most of you did remember to count from 0 rather than 1, but some forgot to do this at the end, when you get down to F_2. Some people wrote down alleged P and Δ that were simply the wrong size.

But the oddest thing was that about eight of you hallucinated a comma after the first 1 in the vector $\mathbf{c}$, and then complained that there were nine entries, not eight. The second entry in $\mathbf{c}$ is $1 - i$.

GKS, 20/6/17