# 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.

You did fairly well in the the pink paper test. Few of you accidentally told me your name or sent me the wrong part of the exam. What you often didn't do was tick the boxes saying which questions you have done, which would be helpful. Instead you dutifully wrote down the serial number of your university calculator, which isn't.
I can't really blame you for this, though. The rubric on the pink paper says that if you do not write down that number you will be pursued by the Eumenides, or have your parking permit revoked, or suffer some equally ridiculous penalty, and naturally you don't want to risk any of those things. I have no idea at all why it says that.

Q2. Most people could do most of this but very few got the last part completely right. It's not difficult but it's not quite what you are used to so you have to think. Not everybody seemed to understand that RSA is a public key system: anybody (including Eve) may use it to send Alice a message. Some of you seem do not realise that the security is all in the knowledge that Alice has about $M$: apart from a very few completely stupid choices she may take $a$ to be just about anything. There is no reason why it shouldn't be her birthday. This mistake didn't cost you anything, though, as the question didn't ask about that.
You do have to say exactly who does what calculation at each stage, how and why. You will also lose marks if you are illogical or imprecise: this is a university mathematics exam. So $m|p$ is not the same thing as $p|m$ and you will not be assumed to have meant one if you wrongly wrote the other: you will be marked down. Likewise $\mathbb{Z}/M$ is not the same thing as $M$. One is a group, the other is a number. You shouldn't really write $\mathbb{F}_M$ either, because $\mathbb{F}_M$ is the field with $M$ elements. That is the same thing as $\mathbb{Z}/M$ if $M$ is prime, but if $M$ is a prime power it exists but is not the same as $\mathbb{Z}/M$ and if $M$ is not a prime power (which it isn't, here) then $\mathbb{F}_M$ doesn't even exist at all.
Speaking of precision, please notice how to spell "receive" (it is written in the question),and take the trouble to learn now the difference between "it's" (meaning "it is" or occasionally "it has") and "its" (meaning "of it"). When you write your CV, people will judge you partly on whether you can write correct English. This mistake, which is made mainly by native speakers, stands out and will create a bad impression.
Although few people got the last part completely right, some did and a few found a solution different from mine and in some ways better, substituting $M/q$ for $p$ and solving

the resulting cubic for $q$. In fact this shows that knowing the value of *any* polynomial in $p$ and $q$ as well as $M$ will allow Eve to break the code.

Q4. This was well done by those who made a serious attempt at it, which wasn't as many as it should have been for this rather easy question. Some of you used the letter $\zeta$ (or some squiggle) without bothering to say what it meant. Some of you multiplied an $n \times n$ matrix by a row vector, with the matrix on the left: you know you can't do that, because a row vector is a $1 \times n$ matrix and you need $n \times 1$. The other thing to remember is that not all fourth roots of unity are $i$.

Q5. Most of you have got the idea of this, although nearly everybody tripped up somewhere. Part (a) of this question does not mention primes, or any specific method. You are not allowed to pretend that it does. Nor are you allowed to assume that $M$ is a group. Even if $M$ does happen to be a group, $(\beta(m)^{-1}$ is not the same thing as $\beta^{-1}(m)$. Most of you avoided these pitfalls in (a) and (b) and then galloped straight into a hole in part (c), which can be answered correctly in one line. A surprising number of people could do (e) but not (d), which is strange because (e) is just (d) only with actual numbers in it. Some forgot which one is the safe prime and which is the Sophie Germain prime. That is understandable, because there is no reason why the names have to be what they are, but (e) gives you a big clue because 23 is prime and 95 isn't. Some of you still think that $q$ is a secret; but it can't be, because Bob and Alice both know it before they start using the system that enables them to tell each other secrets.
Please learn what the words "associative", "distributive" and "commutative" mean and don't use them interchangeably.

GKS, 12/8/12