15-251: Great Theoretical Ideas **Guru:** Anton Bachin

Assignment 5 Common Mistakes Due: A While Ago

0 Miscellaneous (0 points)

We strongly recommend that you read the question and your solution very carefully when you are done typing.

2 Breaking RSA Without Breaking RSA (15 points)

The key parts to this proof:

1. Recognize and correctly represent the information available as a system of congruences.
2. Note that we can assume that all public keys are pairwise relatively prime.
3. Observe that we can apply the Chinese Remainder Theorem (CRT).
4. Correctly state the result from the CRT: a unique solution x *modulo the product of the moduli.*
5. Say that for any student i, $M < n_i$, and thus $M^3 < n_1 \cdot n_2 \cdot \ldots \cdot n_k$.
6. Conclude that $M^3 = x$, so $M = \sqrt[3]{x}$.

If you mentioned each of these ideas, you probably got full credit. Parts (4) and (5) were the most commonly missed steps. You should know that $M^3 \equiv x \pmod{n_1 \cdot n_2 \cdot \ldots \cdot n_k}$ is not the same as $M^3 = x$. It seems that many students still do not understand the idea of a modular congruence, which has a different meaning from "using the mod function."

Both $7 \equiv 2 \pmod 5$ and $7 \bmod 5 = 2$ are true statements. The first is a congruence stating that 7 and 2 have the same remainder when divided by 5. The second uses the "mod function" to say that when you divide 7 by 5, the remainder is 2. However, note that $12 \equiv 7 \pmod 5$ is true, but $12 \bmod 5 = 7$ is false. This is a very important (and somewhat subtle) distinction, and resulted in many incomplete proofs in the homework.

Also, the reason we can find a solution to the system of congruences is that the moduli are pairwise relatively prime, and therefore the Chinese Remainder Theorem guarantees a unique solution $\pmod{n_1 \cdot n_2 \cdot \ldots \cdot n_k}$. Some of you said to just solve the congruences for M^3 using "Gauss's Algorithm." The problem is, how do you know this algorithm will actually work and give you a solution? It actually won't work unless the moduli are pairwise relatively prime, so you need to state that first.

One more small issue: the statement "$n_1, ..., n_k$ pairwise relatively prime" is not equivalent to "$\text{GCD}(n_1, ..., n_k) = 1$." For example, $\text{GCD}(2, 3, 9) = 1$, since there are no factors common to all three, but they are not pairwise relatively prime because $\text{GCD}(3, 9) = 3$.

3 Symmetry Groups (12 points)

In part (a), many students said that we know inverses exist because the identity appears in each row and/or column. The fact that e appears in each row (where e is the identity) implies that for every x there is a y such that $x * y = e$, and the fact that e appears in each column implies that for every x there is a z such that $z * x = e$. But to show that inverses exist, you need to also say that the operation is commutative, so that for every x there is a y such that $x * y = y * x = e$.

4 Pigeons Everywhere (24 points)

In part (a), the possible number of handshakes starts at 0, so there are n possibilites and thus the pigeonhole principle doesn't immediately apply.

In (b), if you want to claim that something like "picking socks so that you make a new pair with every other pick" is the worst case, then you need to prove that too. Otherwise, the best way to do this is to show that no matter what the sequence of picks is, 32 socks is always enough.

In part (c), many people tried to make their pigeons be pairs of disjoint subsets. However, if you do it this way, the pigeonhole principle will only tell you that no matter how you assign the numbers 1...945 to *pairs* of subsets, then two *pairs* will have the same assigned number. This is not the same as saying the two subsets have the same assigned number. Also, a large number of people just forgot to do disjointness – please read the problem carefully!

5 Groups of Functions (16 points)

A surprising number of students composed f and g in part (a), and then neglected to really prove that the composition is in F. In order for the composition to be in F, not only must it have the "form" of a linear function, but the linear coefficient must also be positive! A smaller number of students gave some equations and neglected to make any kind of conclusion from them. If you did not acknowlegde that the first coefficient being positive is necessary for a function to be in F, you lost two points.

Recall that to show that e is an identity element in F, you must show that for every function $f \in F$, $f \circ e = f$ *and* $e \circ f = f$. Many students showed only that one of these is true. There is an analogous requirement for the inverse elements. A different problem in part (b) was that many students derived the inverse and identity elements without any explanation, in somewhat poor style. This often led to the error just described, as the derived elements were not checked against the axioms.

In part (d), some students claimed that F would still be a group if the condition were dropped because they had not used the fact that $a > 0$ in any of their proofs. However, most students correctly described the inverse to a function $f(x) = ax + b$ as $f^{-1}(x) = \frac{x}{a} - \frac{b}{a}$, which can be undefined if a can be zero.

6 Proofs About Groups (18 points)

There are several mistakes which are serious when doing group theory problems. The first is to assume that a group is commutative when performing manipulations. In general, when you move beyond the realm of arithmetic and groups relating to arithmetic over the complex numbers or subsets of the complex numbers, you lose commutativity. $xyxy$ is *not* the same as x^2y^2. This was a major error and resulted in the loss of 3 points. Also, if $t = xy$, then $t^{-1} = y^{-1}x^{-1}$ in general, and when you apply the simplification that $x = x^{-1}, y = y^{-1}$, you are able to correctly derive the answer.

In part (b), a good portion of people started with a definition of commutativity (either $xy = yx$ or $xyx^{-1}y^{-1} = e$) and showed the other is true. If you did this, realize that you haven't shown anything except that these two definitions are equivalent. Again, people performed manipulations where they assumed commutativity (for example, changing the order of a multiplication).

In part (c), people made claims about x raised to any odd power being the identity. This is an instance of not carefully reading the question. Please make sure you understand what the question is stating. Overall, people did very well on this question.