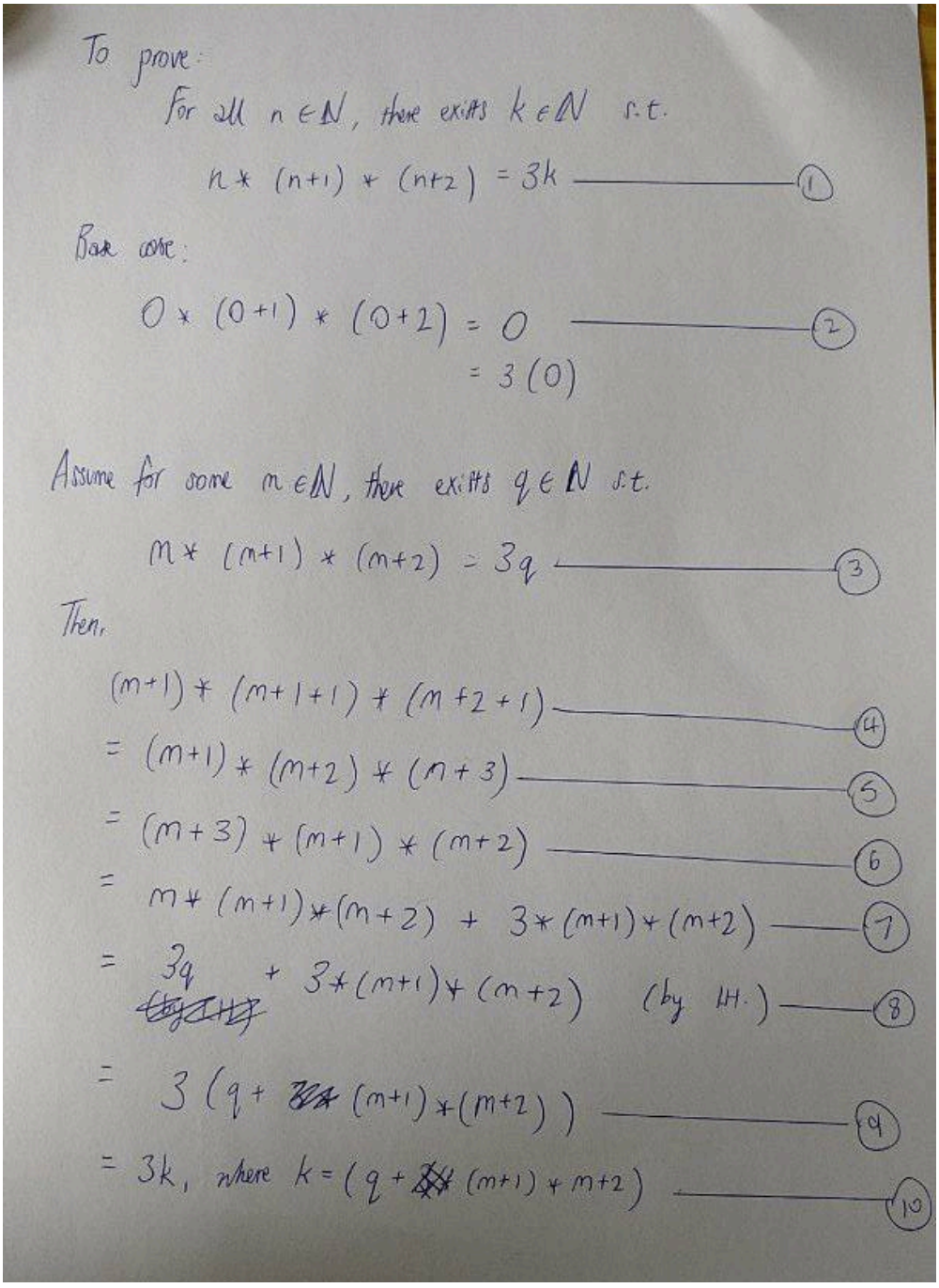
FPP Midterm Report: Additional material

Jeremy Yew

Three consecutive numbers

Handwritten proof:



Comparison with Coq Proof:

- In the base case, the Coq proof requires two rewrites using Nat.mul_0_l due to the default ordering of the multiplication (from left to right). Alternatively, we could apply commutativity to group (1 * 2). The handwritten proof implicitly uses the ordering that is relevant to produce zero in step (2).
- In the Coq proof, the 'natural' name for the inductive case of n is n'. Whereas in the handwritten proof we use a different name (in this case, some m in N, step (3)) out of habit to emphasize that the inductive hypothesis is distinct from the theorem to be proved.
- In addition the Coq proof automatically uses the same existential k in the inductive hypothesis IHn', and automatically generates a distinct name x for the existential only when IHn' is destructured (which we do explicitly). In the handwritten proof we instinctively use a different existential, q, in the inductive hypothesis (at step (3)) to emphasize that it is distinct from k in the theorem.
- The Coq proof requires converting from successor notation to arithmetic notation, and back, in order to use the distributive law of addition, whereas in the handwritten proof this is not necessary. However in the handwritten proof, at step (4), we do explicitly show the addition '+1' instead of implicitly adding the integers, to emphasize the fact that the new terms (m + 1) and so on are the successors of the terms in the inductive hypothesis.
- In the handwritten proof at step (5) to (6) it seemed more natural to move the term (m+3) to the front before distributing, since the first form of the distributive law I thought of was Nat.mul_add_distr_r. This seemed more intuitive as well since we immediately get the term m * (m+1) * (m+2), the same form as the inductive hypothesis. Whereas in the Coq proof, I simply used Nat.mul_add_distr_l immediately, ostensibly to avoid having to rearrange terms until knowing it was absolutely necessary. But in the end I still had to shift n' to the front, and then ungroup the latter two terms using commutativity, before being able to use IHn'. And then later on I also had to move 3 to the front in order to factorize 3 out using the reverse of the distributive law. Thus with handwritten proof we can sometimes 'see ahead' a few steps, and the mental cost of searching and using arithmetic laws is negligible compared to Coq - partly because I haven't fully familiarized myself with the formal statements of the laws, but also because we often combine two Coq steps into one handwritten step, e.g. (5) to (6). This sometimes results in extra unnecessary steps in the Coq proof, the fact of which underlines the benefit of handwriting the proof first. In this case I had initially handwritten the proof very roughly, but only for the sake of knowing the proof method, and did not reflect/plan/reevaluate my Coq steps.