Quiz 9

Math 2001–002, Fall 2016

November 9

Question 1. Make a list of the sentences in the proof below that are claims. For each claim you list, indicate the line on which the demonstration of the claim is completed.

Theorem (Well-ordering principle)**.** *If S is any nonempty set of integers ≥ 0 then S contains a smallest element.*

Theorem. *If n and d are any integers such that $d > 0$ then there are unique integers q and r such that $n = qd + r$ and $0 \leq r < d$.*

Proof. Suppose that n and d are integers such that $d > 0$. We have to prove two things:

1 (i) There are integers q and r such that $n = qd + r$ and $0 \leq r < d$.

2 (ii) If there are integers q, r, q', and r' such that $n = qd+r$ and $n = q'd+r'$ and $0 \leq r < d$ and $0 \leq r' < d$ then $q = q'$ and $r = r'$.

3 We will prove that q and r exist first.

4 There is a set:

$$S = \{n - qd \ : \ q \in \mathbb{Z} \wedge n - qd \geq 0\}$$

5 We will apply the well-ordering principle to S, so we need to verify verify that S is a set of integers ≥ 0 and $S \neq \varnothing$.

6 By definition, S is a set of integers ≥ 0.

7 We need to check that $S \neq \varnothing$.

8 If $n \geq 0$ then $n \in S$, because $n = n - 0d$, so S is not empty.

9 If $n < 0$ then $n - (2n)d = -nd > 0$, so $n - (2n)d$ is in S.

10 Either way, S contains at least one element, so S is not empty.

11 Now we may apply the well-ordering principle to S.

12 Therefore S contains a smallest element, which we will call r.

13 By the definition of S, we know that there is an integer q such that $n - qd = r$.

14 Therefore $n = qd + r$.

15 We still need to check that $0 \leq r < d$.

16 We know that $r \geq 0$ because $r \in S$.

17 On the other hand, r cannot be $\geq d$.

18 This is because $r - d = n - (q+1)d$ and if $r \geq d$ then $r - d \geq 0$, which means $r - d \in S$.

19 Since $r - d < r$, this could only happen if r were not the smallest element of S.

20 To complete the proof, we need to show that the q and r we constructed above are unique.

21 Suppose that $n = qd+r$ and $n = q'd+r'$ where q, r, q', and r' are all integers and $0 \leq r < d$ and $0 \leq r' < d$.

22 Then $qd + r = q'd + r'$.

23 Rearranging this gives

$$(q - q')d = r' - r. \tag{$*$}$$

24 Since $0 \leq r < d$ and $0 \leq r' < d$, we know that $-d < r' - r < d$.

25 Therefore $-d < (q - q')d < d$.

26 Since $d > 0$, we can divide by d to get $-1 < q - q' < 1$.

27 But $q - q'$ is an integer, and the only integer between -1 and 1 is 0.

28 Therefore $q - q' = 0$.

29 Substituting back into ($*$), we get $r' - r = 0$.

30 Therfore $r = r'$, as required.

31 This completes the proof.

Q.E.D.