Math 314 Homework II

Dr. Holmes

September 20, 2009

This assignment is due on Friday the 11th. Visiting me in my office is encouraged!

1. Write a proof of the theorem "the sum of any two odd natural numbers is even" in the same style as the proof of "the product of any two odd natural numbers is odd" in the notes. Of course you need to define "even".

   Solution:

   Definition: A natural number n is said to be *odd* iff there is a natural number k such that $n = 2k + 1$ (or $k + k + 1$).

   Definition: A natural number n is said to be *even* iff there is a natural number k such that $n = 2k$ (or $k + k$).

   Theorem (Main Goal): The sum of any two odd natural numbers is even.

   Rewrite of Main Goal: For any natural numbers m and n, if m and n are odd then $m + n$ is even.

   Let m and n be arbitrarily chosen natural numbers.

   Assume (1): m is odd and n is odd.

   Goal: $m + n$ is even.

   Rephrased Goal: Find k such that $2k = m + n$.
   By (1) we have (2) m is odd and (3) n is odd.
   By (2) we can choose a p such that (4) $m = 2p + 1$.
   By (3) we can choose a q such that (5) $n = 2q + 1$.

Now $m+n=(2p+1)+(2q+1)=2p+2q+2=2(p+q+1)$. Thus, if we define k as $p+q+1$, we have $2k=m+n$, completing the proof.

2. Write a proof of the theorem "the composition of two surjections is a surjection" in the same style as the proof of the theorem about injections in the notes. You may think just of functions from the reals to the reals, as I did in the notes. A function f is surjective (onto the reals) iff for any real y there is a real x such that $f(x)=y$.

   Solution:

Definition: A *surjection* from the reals to the reals is a function f with domain the set of all reals with the property that for any real number y, there is a real number x such that $f(x)=y$.

Theorem (Main Goal): The composition of two surjections (from the reals to the reals) is a surjection.

Rewrite of Main Goal: For any functions f and g from the reals to the reals, if f and g are surjections than $f \circ g$ is a surjection.

Let f, g be arbitrarily chosen functions from the reals to the reals.

Assume (1): f and g are surjections.

Goal: $f \circ g$ is a surjection.

Rewritten Goal: For any real number y, there is a real number x such that $(f \circ g)(x)=f(g(x))=y$.

Let y be an arbitrarily chosen real number.

Goal: Find x such that $f(g(x))=y$.

Discussion: I'm going to do this by finding u such that $f(u)=y$, then finding x such that $g(x)=u$.

By (1) we have (2) f is surjective and (3) g is surjective.

From (2) and the definition of surjection, we have that (4) for any b there is an a such that $f(a)=b$.

From (3) and the definition of surjection, we have that (5) for any c there is a d such that $g(c)=d$.

By (4) we can choose u such that $f(u)=y$.

By (5) we can choose x such that $g(x)=u$.

But then $(f \circ g)(x)=f(g(x))=f(u)$, so the proof is complete: we have found the x we are looking for.

3. Prove two of the following familiar theorems of Peano arithmetic. If you prove more you might get extra credit. You may assume the theorems proved in the notes, and you may assume the associative law of addition, which I also proved in class. I may add that proof to the notes eventually.

   It is quite possible that the order in which I have given these is not the best order in which to try to prove them. You may want to prove special lemmas as I did in the proof of commutativity of addition.

   In the solutions I change the order of the parts so that the associative law, whose proof seems to require distributivity, appears after distributivity.

   (a) the commutative law of multiplication

   Theorem (Main Goal): For all natural numbers m and n, $m \cdot n = n \cdot m$.

   Let m be an arbitrarily chosen natural number.

   Goal: For any natural number n, $m \cdot n = n \cdot m$.

   We prove this goal by mathematical induction.

   Basis Goal: $m \cdot 0 = 0 \cdot m$

   We prove this by proving a lemma.

   Lemma 1: For all natural numbers x, $x \cdot 0 = 0 \cdot x$.

   We prove this by mathematical induction. Notice that if we prove this, we immediately establish the Basis Goal of the main proof.

   Basis Goal (for Lemma 1): $0 \cdot 0 = 0 \cdot 0$

   This follows from logic (reflexive property of equality).

   Induction Step for Lemma 1: Let k be an arbitrarily chosen natural number.

   Assume (ind hyp): $0 \cdot k = k \cdot 0$

   Induction Goal: $0 \cdot S(k) = S(k) \cdot 0$

   $0 \cdot S(k) =$(IX)$0 \cdot k + 0 =$(VI)$0 \cdot k =$(ind hyp)$k \cdot 0 =$(VIII)$0 =$(VIII)$S(k) \cdot 0$.

   Induction Step: let k be an arbitrarily chosen natural number.

Assume (ind hyp): $m \cdot k = k \cdot m$

Induction Goal: $m \cdot S(k) = S(k) \cdot m$

$m \cdot S(k) =$(IX)$m \cdot k + m =$(ind hyp)$k \cdot m + m =$(???)$S(k) \cdot m$.

We justify the last equation by proving another lemma.

Lemma 2: For any natural number x, $k \cdot x + x = S(k) \cdot x$

We will prove Lemma 2 by mathematical induction. Notice that once the lemma is proved the unjustified step in the main proof will be justified and the main proof will be complete. Notice that in the current context, m and k are fixed arbitrarily chosen numbers: for this reason we will use a different induction variable below.

Basis Goal (for Lemma 2): $k \cdot 0 + 0 = S(k) \cdot 0$

$k \cdot 0 + 0 =$(VI)$k \cdot 0 =$(VIII)$0 =$(VIII)$S(k) \cdot 0$

Induction Step (for Lemma 2): Let y be an arbitrarily chosen natural number (we use y because k is already in use [and actually appears in what we are proving!]).

Assume (ind hyp): $k \cdot y + y = S(k) \cdot y$

Induction Goal: $k \cdot S(y) + S(y) = S(k) \cdot S(y)$

$S(k) \cdot S(y) =$(IX)

$S(k) \cdot y + S(k) =$(ind hyp)

$k \cdot y + y + S(k) =$(successor is same as adding one)

$k \cdot y + y + k + 1 =$(known regrouping properties of addition)

$k \cdot y + k + y + 1 =$(successor is same as adding one)

$k \cdot y + k + S(y) =$(IX)

$k \cdot S(y) + S(y)$

(b) the distributive law of multiplication over addition (you might want to consider the left and right distributive laws separately if you do not prove commutativity of multiplication first).

I note here in the solutions that I will accept one of the two distributive properties as complete work for this part. I will give proofs for both.

I am giving these proofs with less detail than the commutativity proof. You are welcome to ask in class or in my office for the details (the logical frame is given with somewhat less detail; each step in the equational calculations is justified by an axiom or by previously proved results, but the justification is usually not given; it is a good exercise for you to supply the justifications). Notice that I *always* label use of the inductive hypothesis, and I expect this of you.

Theorem 1 (Main Goal): $x(y+z) = xy + xz$

Comment: You really want to prove this by induction on z, not x. It is almost always better (because of the way we set up the axioms) to work with the variable appearing farthest to the right.

Basis Goal: $x(y+0) = xy + x0$

$x(y+0) = xy = xy + 0 = xy + x0$

Assume (ind hyp): $x(y+k) = xy + xk$

Induction Goal: $x(y+S(k)) = xy + xS(k)$

$x(y+S(k)) = x(S(y+k)) = x(y+k)+x =$(ind hyp)$xy+xk+x = xy + xS(k)$

Theorem 2 (Main Goal): $(x+y)z = xz + yz$

This is the other version of the distributive property.

Basis Goal: $(x+y)0 = x0 + y0$

$(x+y)0 = 0 = 0 + 0 = x0 + y0$

Assume (ind hyp): $(x+y)k = xk + yk$

Induction Goal: $(x+y)S(k) = xS(k) + yS(k)$

$(x+y)S(k) = (x+y)k + (x+y) =$(ind hyp)$xk + yk + x + y = (xk + x) + (yk + y) = xS(k) + yS(k)$

(c) the associative law of multiplication

I am giving this proof with less detail than the commutativity proof. Same comments as on the distributivity proofs.

Theorem (Main Goal): $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

Basis Goal: $(x \cdot y) \cdot 0 = x \cdot (y \cdot 0)$

$(x \cdot y) \cdot 0 = 0 = x \cdot 0 = x \cdot (y \cdot 0)$

Assume (ind hyp): $(x \cdot y) \cdot k = x \cdot (y \cdot k)$

Induction Goal: $(x \cdot y) \cdot S(k) = x \cdot (y \cdot S(k))$

$(x \cdot y) \cdot S(k) = (x \cdot y) \cdot k + (x \cdot y) =$(ind hyp)$x \cdot (y \cdot k) + x \cdot y =$(distributivity!)$x \cdot (y \cdot k + y) = x \cdot (y \cdot S(k))$