Tutorial on reasoning about recursion in Java

Q You said in your lecture that reasoning about recursion in Java was just like in Haskell. I tried to reason about gcd but I'm finding it hard. Could you help?
A Where exactly are you stuck?
Q I showed the base case when y=0. That is, I showed the result (=x) satisfies
x≥0 & x|0 & x|x & □z:int(z|x & z|0 -> z|x).

I used the definition of "|", that z|x if x=m*z for some int m.
Most of the properties are easy: x|0 because 0*x=0.

But I am not sure what the Ind. Hyp. should be.
A You want to show that for any non-negative x and y the post-condition holds. Since you appear to be using induction on y ....
Q I see – I let
P(y) be □x:nat(r≥0 & r|x & r|y & □z:int(z|x & z|y -> z|r),where r=gcd(x,y).
I can assume P(y′) for all 0<y′<y and try to show P(y) ...
A You don’t seem to need me after all!
Q Let x>0 be an arbitrary int.

How do I know what r is?
A Use the program.
Q Oh yes, of course.

Since y>0, r=gcd(x,y)=gcd(y,x%y).
As x%y<y I can use the Hyp.
A Why is x%y<y? Also, you need that x%y>0 to use the hypothesis.
Q OK! A property of "%" is that 0=x%y<y.

So then I can deduce from the hypothesis that
r≥0 & r|y & r|x%y & □z:int(z|y & z|x%y -> z|r)

And I have to show (i) r|x, and (ii) r|y and (iii) □z:int(z|x & z|y -> z|r).

(iii) is true from the hypothesis.

I think I am stuck for sure now as the hypothesis doesn’t seem to apply.
A You give up too easily.
Call x%y = g and write down a property involving x, y and g.
Q Mmmm. g+k*y=x?
A Correct.
Q Ah! I see. Then this property holds also:
for any z:int if z|g and z|y then z|x, and if z|x and z|y then z|g (**).

When I take r for z, I can deduce (i) from the hypothesis.
To show (iii), suppose that z|x and z|y. Then z|x%y follows by (**).
Therefore z|y and z|x%y so z|r, which is what I want.

I think it’s done!
A Excellent. (KB Feb 2002)